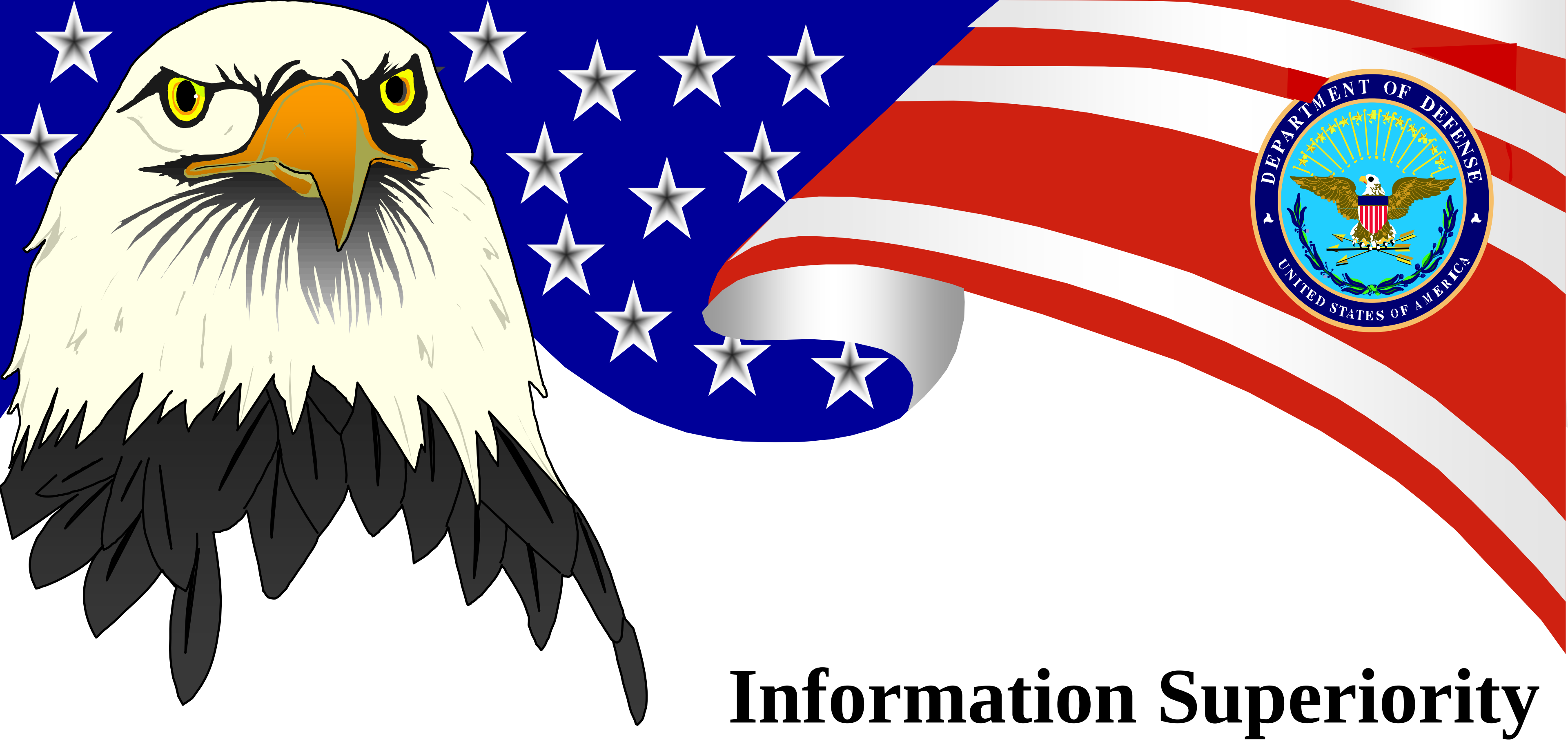


Information Superiority
&
the Future of DoD

- Opportunities, Risks, and Challenges -

Prepared by the
Office of the Assistant Secretary of Defense (C3I)
POC: Dr. David S. Alberts -- Director, Research and Strategic Planning

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
JAN 2001

2. REPORT TYPE

3. DATES COVERED
00-00-2001 to 00-00-2001

4. TITLE AND SUBTITLE
Information Superiority & the Future of DoD -Opportunities, Risks, and Challenges-

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Office of the Assistant Secretary of Defense (C3I),Research and Strategic Planning,Washington,DC,20330

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**180**	

Instructions for Slide Show Mode

- This briefing has been designed to be “interactive” in Slide Show mode
- Slide Show mode is found under “view”
- ● Indicates there are “drill down” slides available - to view these click on this symbol
- click **more** ⇨ to continue with drill down slides
- click ⇦ **back** to return to the previously viewed slide
  click
- click ⤴ **Agenda** to return to the Agenda slide
- click ⤴ ● to return to the slide from which you began the drill down

Re: Printing -- Please note that for some reason some printer drivers “move” these link symbols to places other than where they appear on the screen.

Agenda

- Bottom Line Assessment
- Information Superiority: the critical enabler
- From Shortfalls to Recommendations
- Critical Shortfalls
- What Needs to be Done

Drill Down Sections

- Transformation / JV2020
- Information Superiority
- Building Blocks of IS
- Network Centric Warfare
- Network Centric Enterprise (e-Business)
- IS/NCW Research, Analysis, and Exp'ts
- Impediments and Challenges
- Issues and Recommendations

All

A Bottom Line Assessment

Agenda

Future military concepts and operations are predicated on Information Superiority

Problems *(remain despite significant accomplishments to date)*

- Our networks and infrastructures are vulnerable and fragile
- We are unable to provide the Information Superiority needed to
  - support the warfighter today
  - support emerging operational concepts (RMA)
  - enable business process improvement and re-engineering (RBA)

Reasons

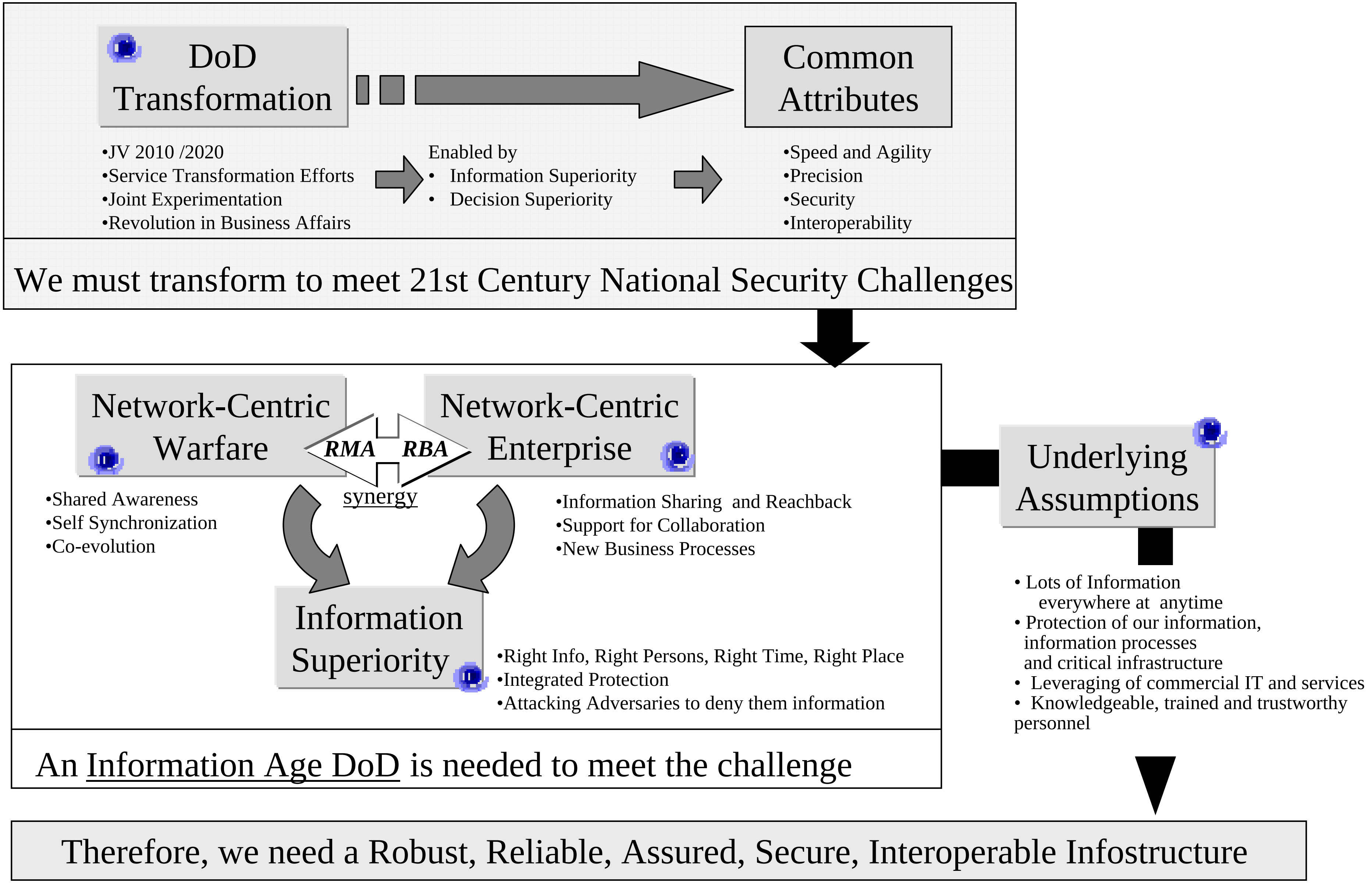
- Program of record
  - is too slow to deliver needed capabilities
  - will not provide sufficient Information Superiority capabilities needed for JV2020 and Service transformation goals
- Fragmented authorities and stove-piped processes are antithetical to a seamless flow of info
- Policy, Process, Personnel, Technology, and Materiel are not properly aligned

Bottom Line → ***U.S. Forces and DoD transformation are at Risk !!***

Information Superiority: the critical enabler

An imbalance in one’s favor in the Information Domain *JV2020*

Agenda



DoD Transformation

Common Attributes

- JV 2010 /2020
- Service Transformation Efforts
- Joint Experimentation
- Revolution in Business Affairs

Enabled by

- Information Superiority
- Decision Superiority

- Speed and Agility
- Precision
- Security
- Interoperability

We must transform to meet 21st Century National Security Challenges

Network-Centric Warfare

RMA *RBA*

synergy

Network-Centric Enterprise

- Shared Awareness
- Self Synchronization
- Co-evolution

- Information Sharing and Reachback
- Support for Collaboration
- New Business Processes

Information Superiority

- Right Info, Right Persons, Right Time, Right Place
- Integrated Protection
- Attacking Adversaries to deny them information

An Information Age DoD is needed to meet the challenge

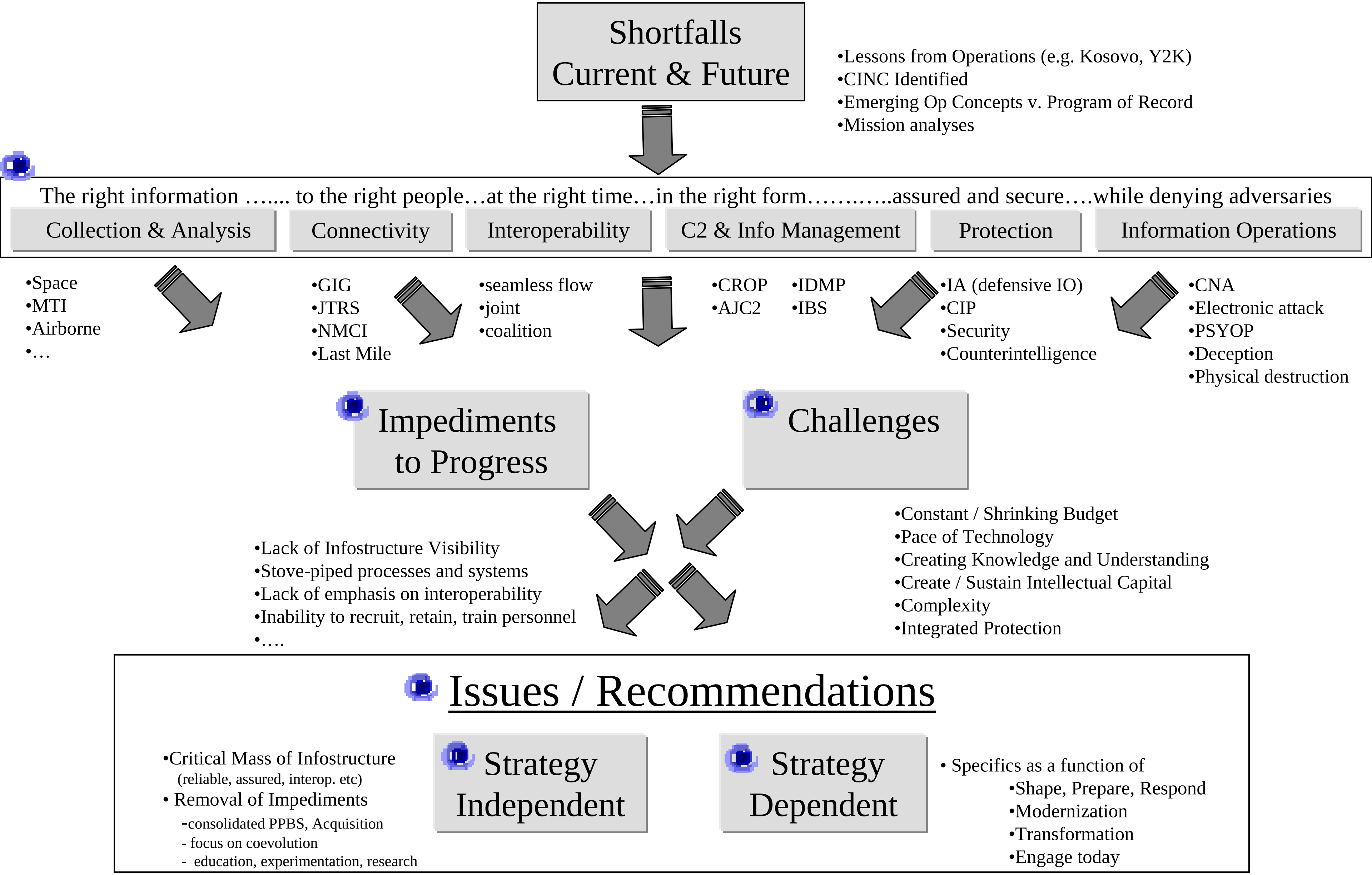
Underlying Assumptions

- Lots of Information everywhere at anytime
- Protection of our information, information processes and critical infrastructure
- Leveraging of commercial IT and services
- Knowledgeable, trained and trustworthy personnel

Therefore, we need a Robust, Reliable, Assured, Secure, Interoperable Infostructure

From Shortfalls to Recommendations

Agenda



Shortfalls
Current & Future

- Lessons from Operations (e.g. Kosovo, Y2K)
- CINC Identified
- Emerging Op Concepts v. Program of Record
- Mission analyses

The right information ….... to the right people…at the right time…in the right form………..assured and secure….while denying adversaries

Collection & Analysis | Connectivity | Interoperability | C2 & Info Management | Protection | Information Operations

- Space
- MTI
- Airborne
- …

- GIG
- JTRS
- NMCI
- Last Mile

- seamless flow
- joint
- coalition

- CROP
- AJC2

- IDMP
- IBS

- IA (defensive IO)
- CIP
- Security
- Counterintelligence

- CNA
- Electronic attack
- PSYOP
- Deception
- Physical destruction

Impediments
to Progress

Challenges

- Lack of Infostructure Visibility
- Stove-piped processes and systems
- Lack of emphasis on interoperability
- Inability to recruit, retain, train personnel
- ….

- Constant / Shrinking Budget
- Pace of Technology
- Creating Knowledge and Understanding
- Create / Sustain Intellectual Capital
- Complexity
- Integrated Protection

Issues / Recommendations

- Critical Mass of Infostructure
  (reliable, assured, interop. etc)
- Removal of Impediments
  - consolidated PPBS, Acquisition
  - focus on coevolution
  - education, experimentation, research

Strategy
Independent

Strategy
Dependent

- Specifics as a function of
  - Shape, Prepare, Respond
  - Modernization
  - Transformation
  - Engage today

Critical Shortfalls

Agenda

	People	Policy / Process	Technology / Material
IA and CIP	•system administrators •IA awareness & training •computer specialists	•risk & network mgt •integrated warfighter CIP rqts •legal framework •Public/Private Sector partnerships	•attack sensing and warn'g •defense-in-depth •secure COTS •PKI scalability
GIG	•IT professionals •information managers •architects & integrators	•network-centric management •rqts / finance / acquisition •national spectrum mgt •plug and play	•Interoperability •configuration mgt •BLOS comms •joint tactical comms
C3ISR	•C2 career path •info mgt career path	•integrated develop / acq •overhead /airborne integration	•improved sensors •sensor TPED •plug and play
Knowledge	•shared intellectual capital •incentives to collaborate	•information management •knowledge management •collaborative processes	•basic C2 research • tools - decision aids - assimilation - collaboration
Intelligence	•language specialists •analysts •collectors	•integrate DoD/DCI priorities •multi-int TPED •coalition sharing	•Intel fidelity for IO •SIGINT •MASINT
Security & CI	•security awareness • cyber investigators	•new security paradigm •integrated protection •personnel security •proactive CI	•data mining •assimilation •CI correlation/ analysis •Interop of IA services
RBA/EB	•IT awareness •change agents	•CIO acceptance •process change •e-Business	• enterprise network
Info Ops	•IO career path	•end-to-end deliberate planning •IO integration w/ ops •PSYOPS/EW •Overprotection •Intel support	• CNA tools •Measures of effectiveness

What needs to be done

Agenda

- Keep the Momentum going
  - Global Information Grid (GIG)
  - Defense-in-Depth
  - Counter-Intelligence (CI-21)
  - High Density / Low Density Assets
  - Responsive Personnel Security

- accelerate
  - IS-related Experimentation
  - Information Management
  - Common Relevant Op Picture
  - C2 Research & Analysis
  - Strategic Planning

- Tackle some stubborn problems

  Recruit, Train, Retain
  - Infostructure Visibility
  - Intel Priorities / Shortfalls
  - Joint / Coalition Interoperability

  Architectures / Standards
  - Integrated Protection
  - Space Surveillance

  Last Mile
  - Counters to Insider Threat
  - System of System Integration
  - Technical Security Challenges
  - Critical Infrastructure Protection

- Work for reforms needed to support transformation
  - CIO Authorities

  IT Requirements process

  Title 10

  IT Acquisition Reform

  Goldwater Nichols II
  - Leveraging Commercial
  - Cost-based Accounting
  - e - Business / Knowledge Mgt

  Personnel Reform

Drill Downs

Drill Downs

Transformation
&
Joint Vision 2020

DoD Transformation

Agenda
back
more

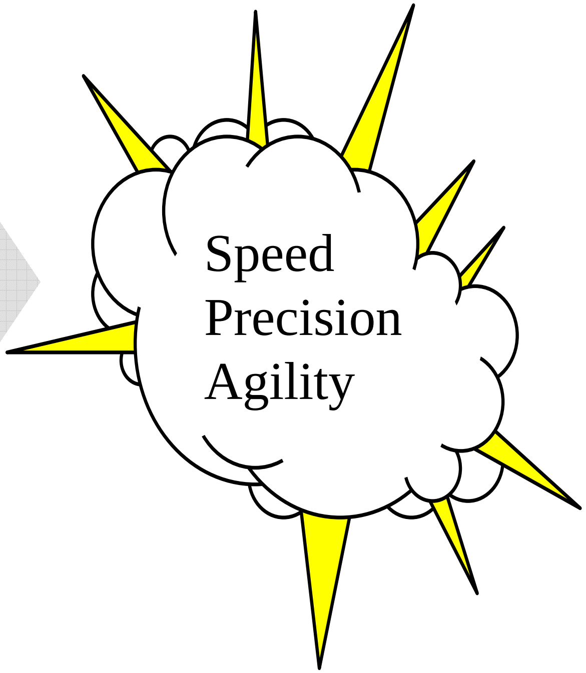
Transformed Military forces are needed because the strategic environment is changing

Transformed Military forces are possible because of the RMA / RBA

- ***Joint Vision 2020*** for Full Spectrum Dominance
  - Dominant Maneuver
  - Precision Engagement
  - Focused Logistics
  - Full-dimensional Protection
- Service Transformations all envision
  - Rapid deployment
  - Decisive operations
  - Agile forces
  - Responsive logistics
  - Rapid, adaptive planning and execution

Agenda

- Joint Experimentation for the next level of Jointness
  - Adaptive Joint command and control
  - Joint interactive planning
  - Common relevant operational picture
  - Information Operations



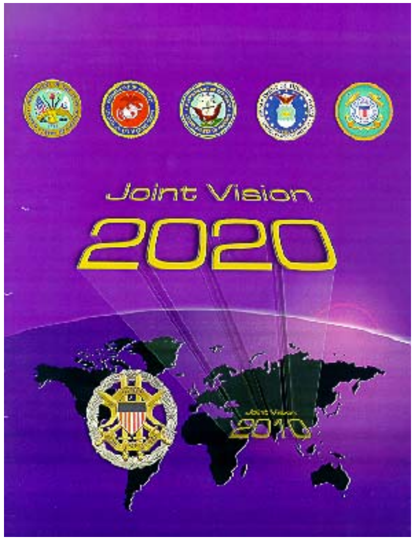
Speed
Precision
Agility

Joint Vision 2020

Agenda

back

more



Full Spectrum Dominance

Enhanced Operational Concepts

Dominant Maneuver
Precision Engagement
Focused Logistics
Full Dimension Protection

Information Operations

Joint Command and Control

Multinational and Interagency Operations

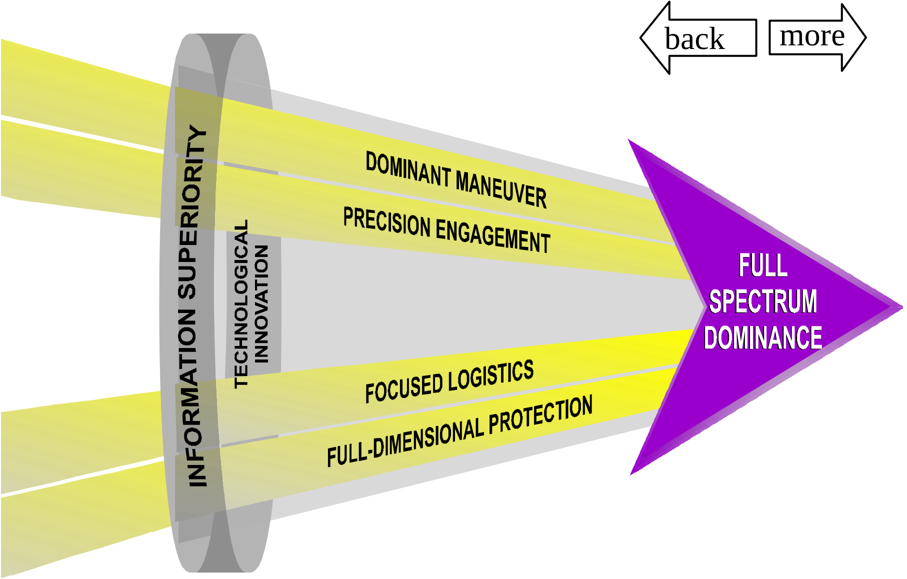
Decision Superiority

Information Superiority

People

Innovation

Interoperability



Underlying Assumptions

Agenda
back
more

- *The Emerging Concepts of Operation assumes that we will be able to:*
  - *maintain a high level of situational awareness*
  - *create shared awareness and knowledge across the battlespace*
  - *plan and execute dynamically*

- *Embedded in these assumptions are a new way of doing business*
  - *a networked Force*
  - *a high level of situational awareness and knowledge*
  - *shared awareness across the coalition battlespace*
  - *dynamic planning and execution*

- *To support a new way of doing business we must be able to:*
  - *access all available information*
  - *protect our information, information processes and critical infrastructure*
  - *leverage commercial IT and services*
  - *recruit, retain, train knowledgeable personnel*

If we continue on the current course these Assumptions will NOT be met !!

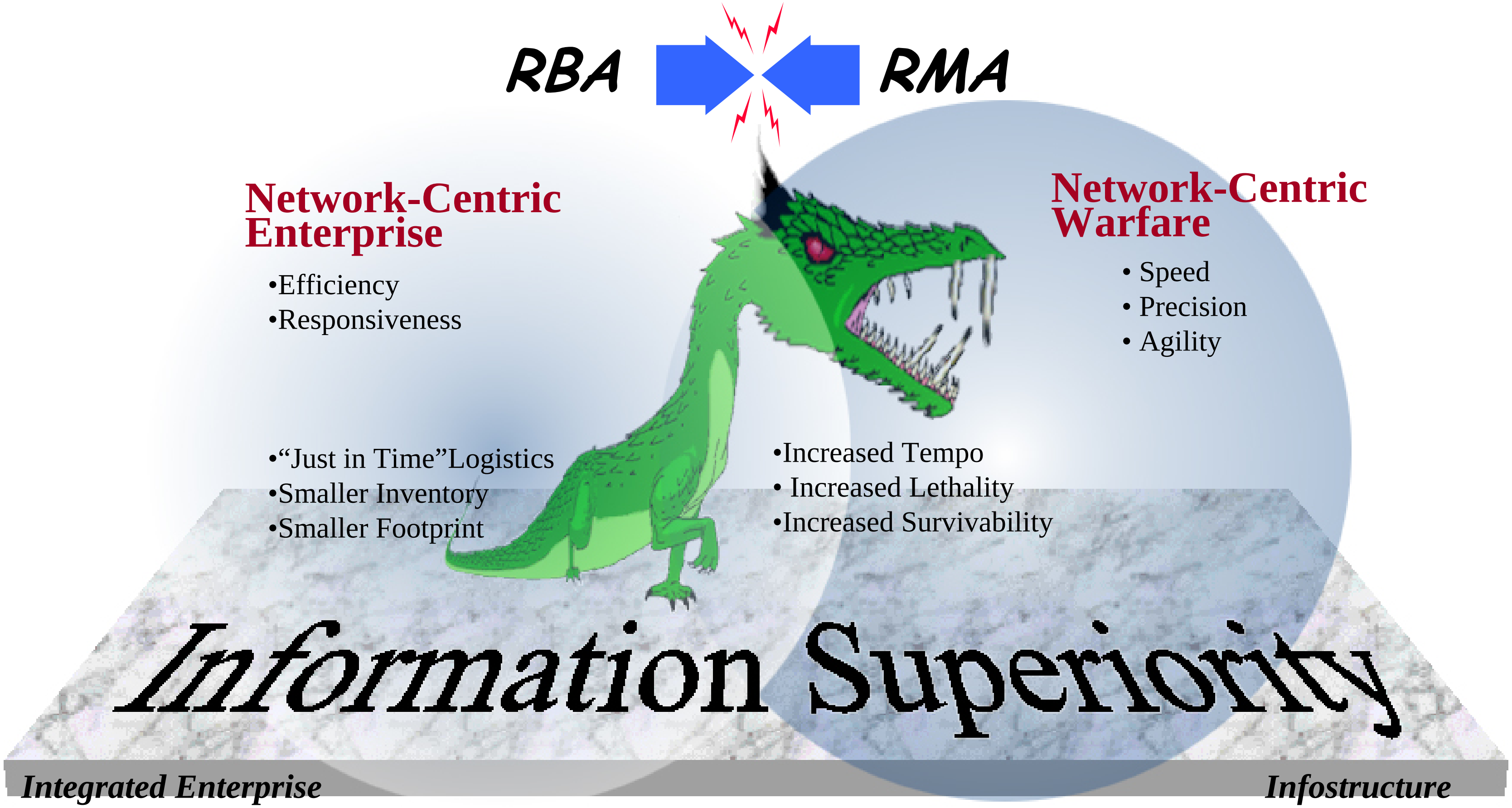
Information Age DoD

- Information-Driven v. Uncertainty-Driven
- Integration Across Several Dimensions
  - Time (Simultaneity)
  - Echelons
  - Functions
  - Geography
  - Coalitions
- Self Organizing & Synchronizing Forces

RBA & RMA Synergy

Agenda

back



RBA

RMA

Network-Centric Enterprise

- Efficiency
- Responsiveness

- “Just in Time”Logistics
- Smaller Inventory
- Smaller Footprint

Network-Centric Warfare

- Speed
- Precision
- Agility

- Increased Tempo
- Increased Lethality
- Increased Survivability

Information Superiority

Integrated Enterprise

Infostructure

In a network-centric force, everyone is on the frontlines

Drill Downs

Information Superiority

INFORMATION SUPERIORITY : *What it is?*

Agenda
back
more

The

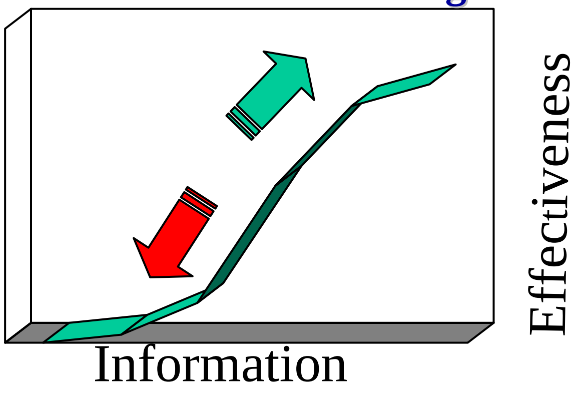
RIGHT

Information from Sources to People at Time and Place in Format. ***DPG***

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. ***DPG and Joint Pub 3-13***

Information Overload

The Information Edge

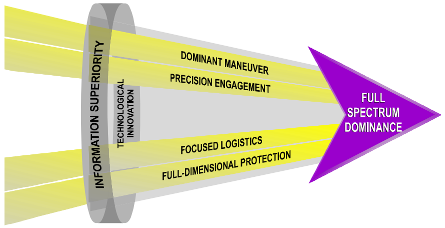


Seamless Joint and Combined Interoperability

Assured Information on Demand Anywhere in Real Time with Zero Error

Different Perspectives, the Same Bottom Line: More for Us; Less for Them

relative to one's information needs



Joint Vision 2010: The band where the miracle happens.

An imbalance in one's favor in the information domain

Key INFORMATION SUPERIORITY Concepts

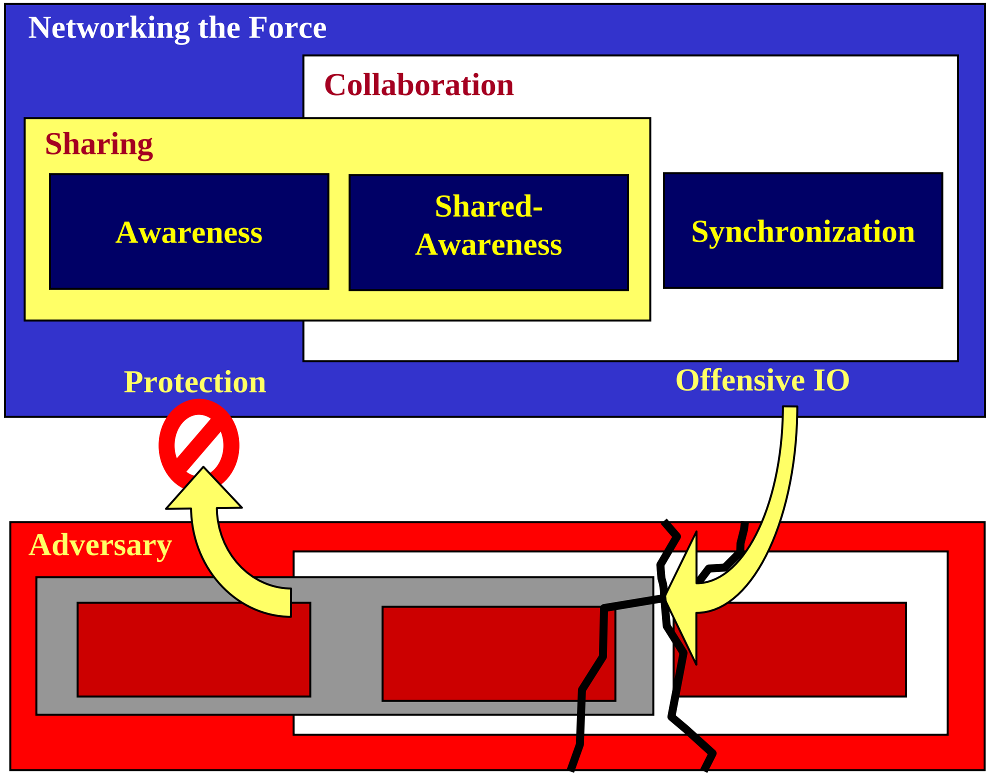
Agenda
back
more

A State achieved by establishing a
Relative Information Advantage
from which a
Competitive Advantage
can be gained.

1. Getting the Right Information to the Right People at the Right Times in the Right Forms

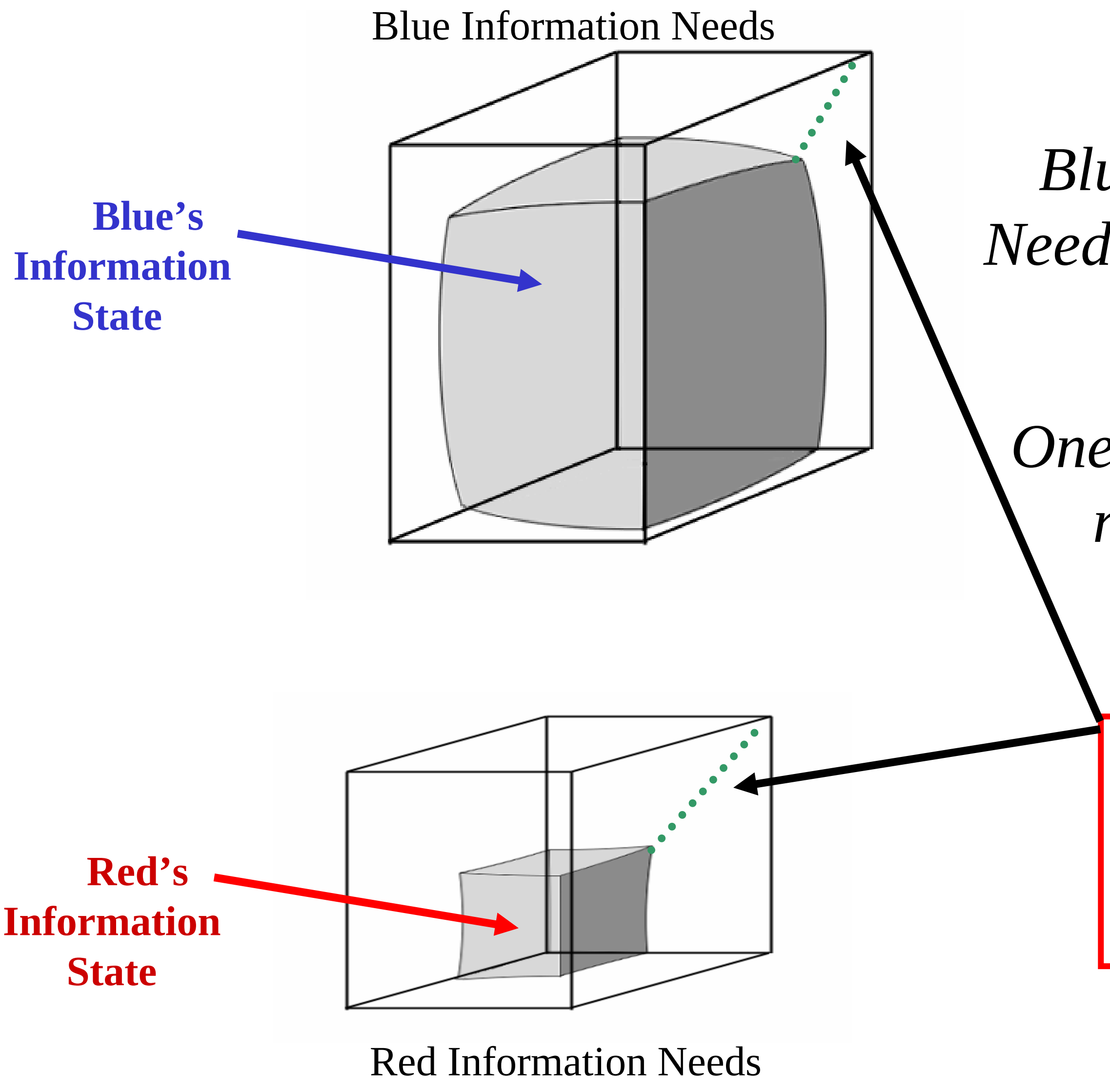
2. Protecting our Information and Information Processes

3. Preventing our Adversaries from doing the same



Relative Information Position

Agenda
back
more



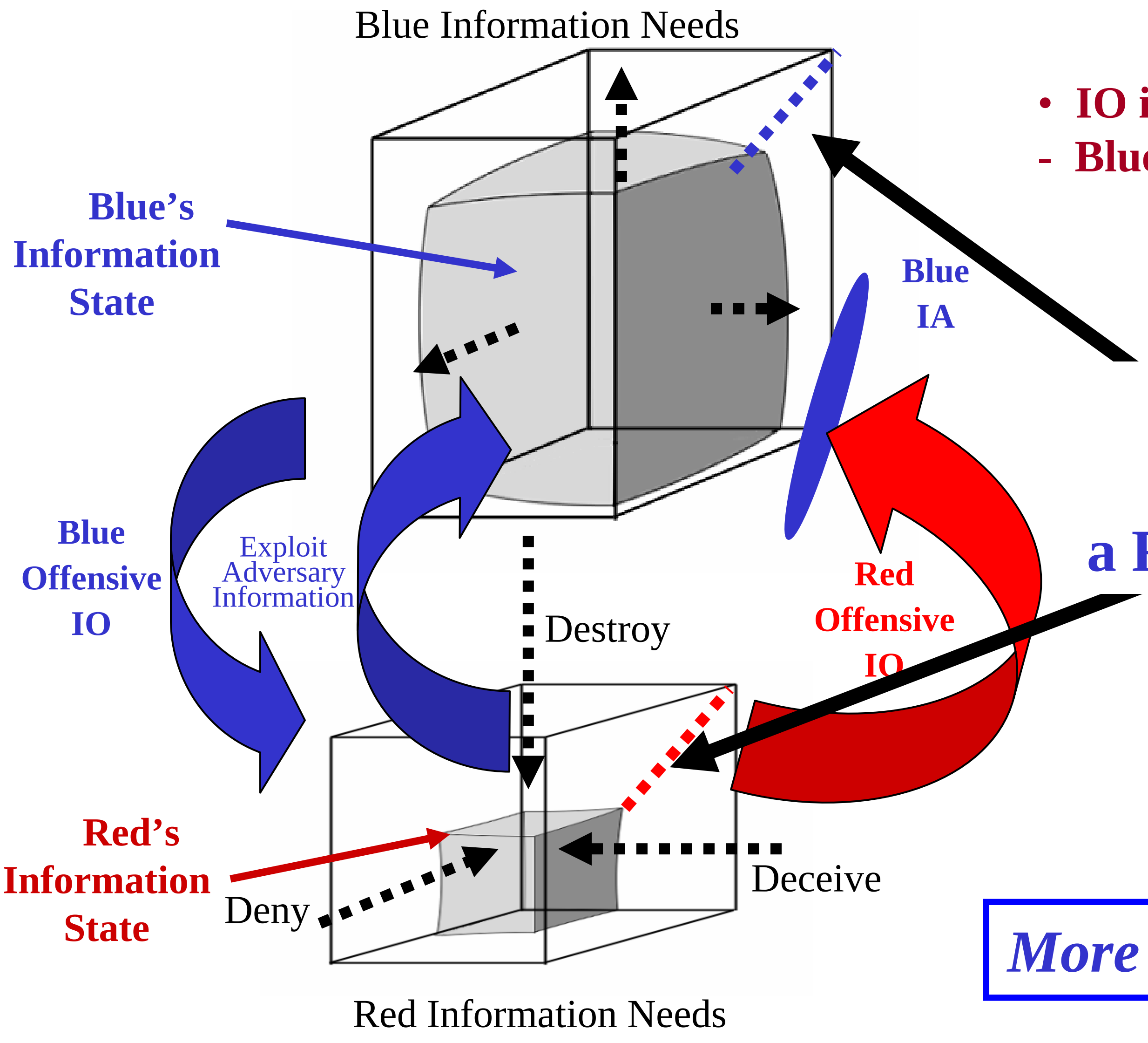
Blue and Red Information Needs are potentially different

One's Information position is relative to one's Needs

The Objective is to Improve Blue's Relative Information Position Vs Red's Relative Information Position

Impact of Information Operations

Agenda
back
more



Blue Information Needs

Blue's Information State

Blue IA

Blue Offensive IO

Exploit Adversary Information

Destroy

Red Offensive IO

Red's Information State

Deny

Deceive

Red Information Needs

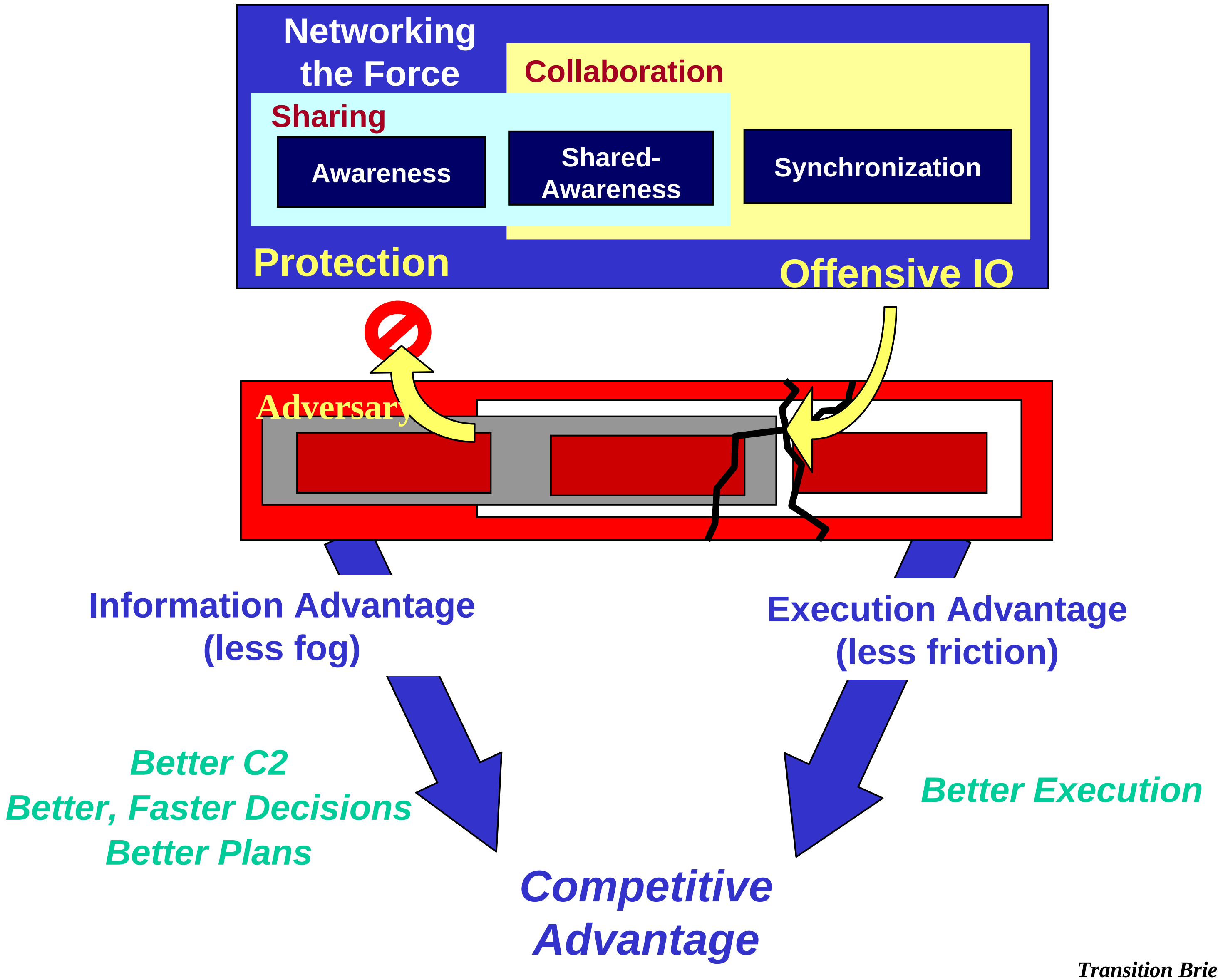
- **IO is Dynamic and N-Sided**
- **Blue, Red, Others (e.g. CNN)**

IO Works to Enhance and Protect a Relative Info Advantage

More for us is not enough

Value Chain

Agenda
back
more



Networking the Force

Collaboration

Sharing

Awareness

Shared-Awareness

Synchronization

Protection

Offensive IO

Adversary

Information Advantage
(less fog)

Execution Advantage
(less friction)

Better C2
Better, Faster Decisions
Better Plans

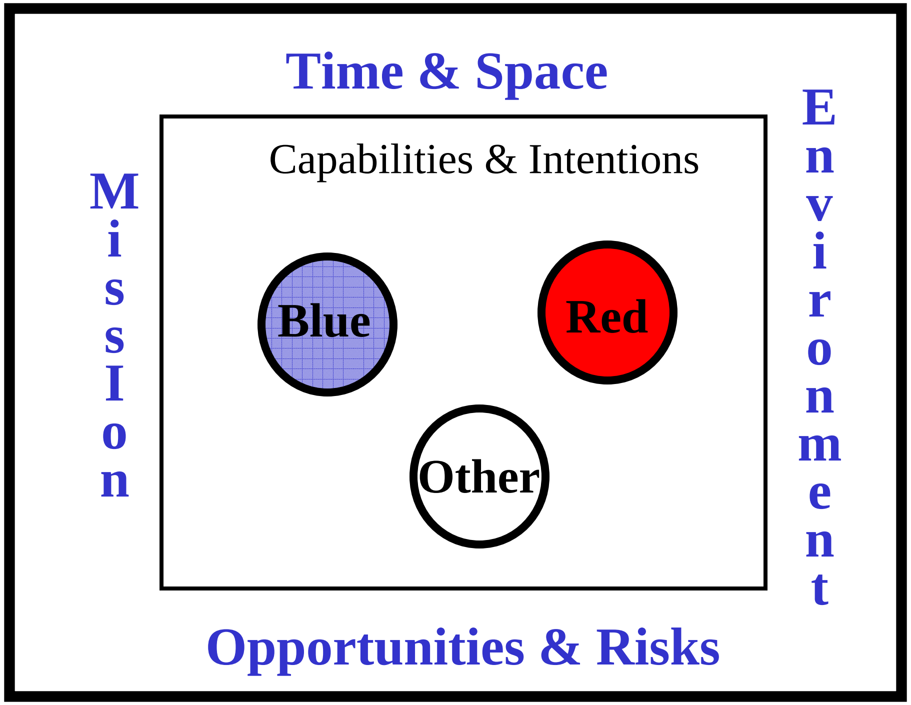
Better Execution

Competitive Advantage

Awareness

- Awareness is a Perception of the Situation

The Situation



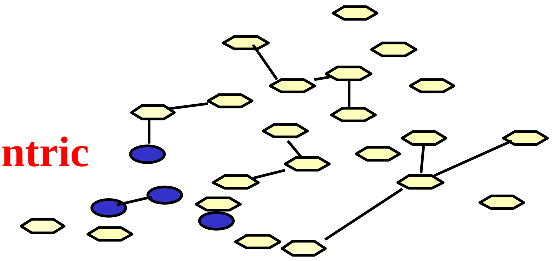
- Levels of Awareness
  - entities, relationships, the patterns and implications

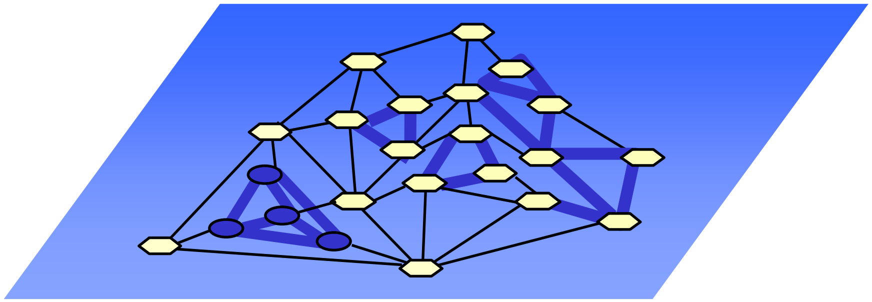
Sharing

Agenda
back
more

- Sharing Lies at the Core of IS & NCW
  - Creates Increased Awareness
  - Creates Shared Awareness
- Entry Fee is the “Network” (for the DoD it’s the GIG)
- Sharing Has an Organizational, a Behavioral, and a Technical Component
  - Interoperability v. Cooperability
  - Technical Component Enables
  - Organizational and Behavioral Components Generate Value

Platform-Centric





Network-Centric

A Basic Paradigm Shift in Dealing With *Information*

Collaboration

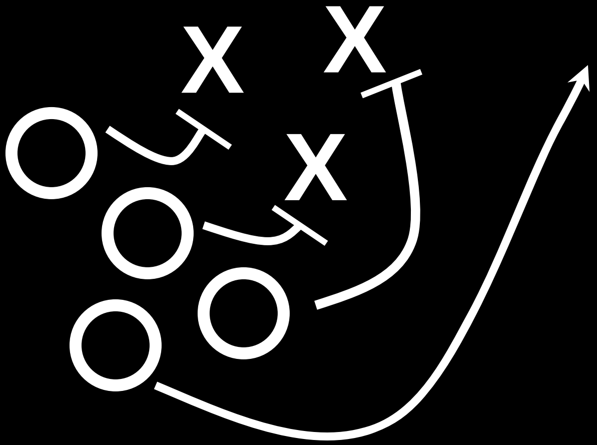
Agenda
back
more

- Collaboration requires Shared Awareness
- Collaboration in the Information and Cognitive Domains Creates an *Information* Advantage
- Collaboration in the Warfighting Domain Creates Value by Exploiting an *Information* Advantage to Create a Competitive Advantage
- Collaboration Takes Places “on the Net”or is Reflected “in the Net”
- The Ability to Share Awareness Creates New Forms of Collaboration (e.g., Self-Synchronization)

Synchronization

“Purposeful arrangement of things in time and space.”

- Synchronization is an output characteristic of a command and control process that *arranges and continually adapts* the relationships of military actions in time and space to achieve the objective
- Fuses the information, cognitive, and physical domains
- Involves a dynamic component that orchestrates relationships among many dimensions:
  - Time (sequencing)
  - Space (simultaneity)
  - Purpose Level (Strategic, Operational, Tactical)
  - Arenas (Air, Land, Sea, Space, Cyberspace)
  - Organizational Synchrony


X
X
X
O
O
O
O

TELE+
EUROCARD

11

La Lechera

Drill Downs

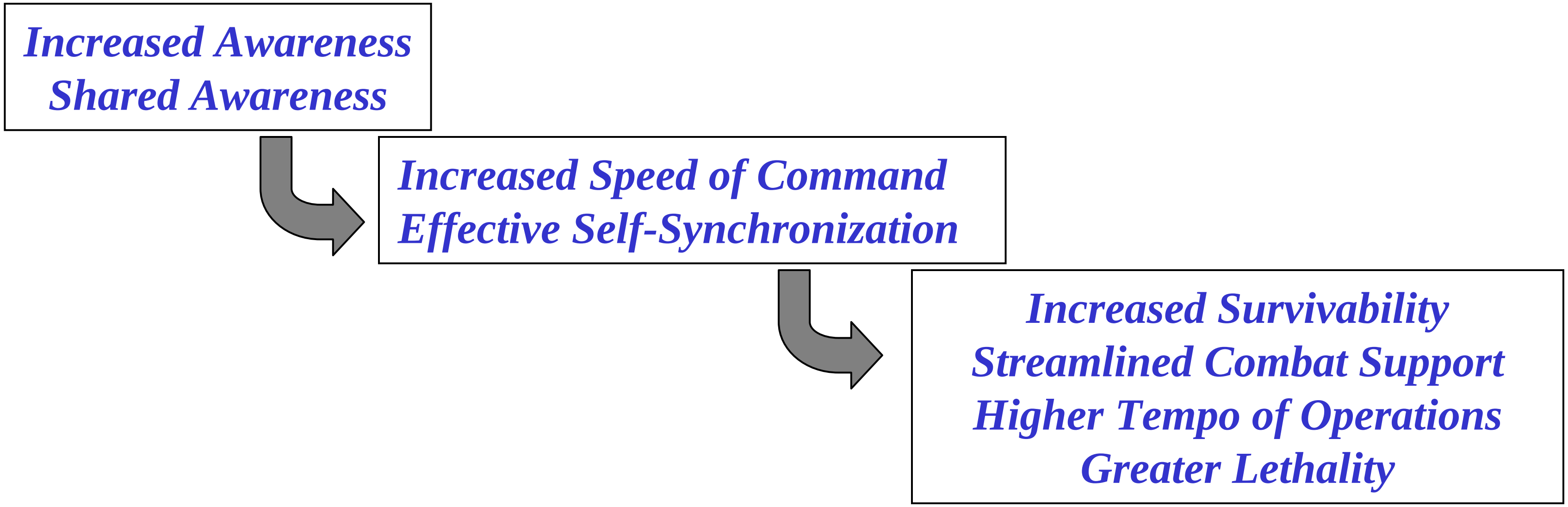
Network Centric Warfare

Network Centric Warfare

Agenda
back
more

Network Centric Warfare Translates Information Superiority into Combat Power

A Warfighting Concept
that Enables a Network Centric Force
(Robustly Networked Sensors, Decision Makers, and Shooters)
to Significantly Increase Combat Power



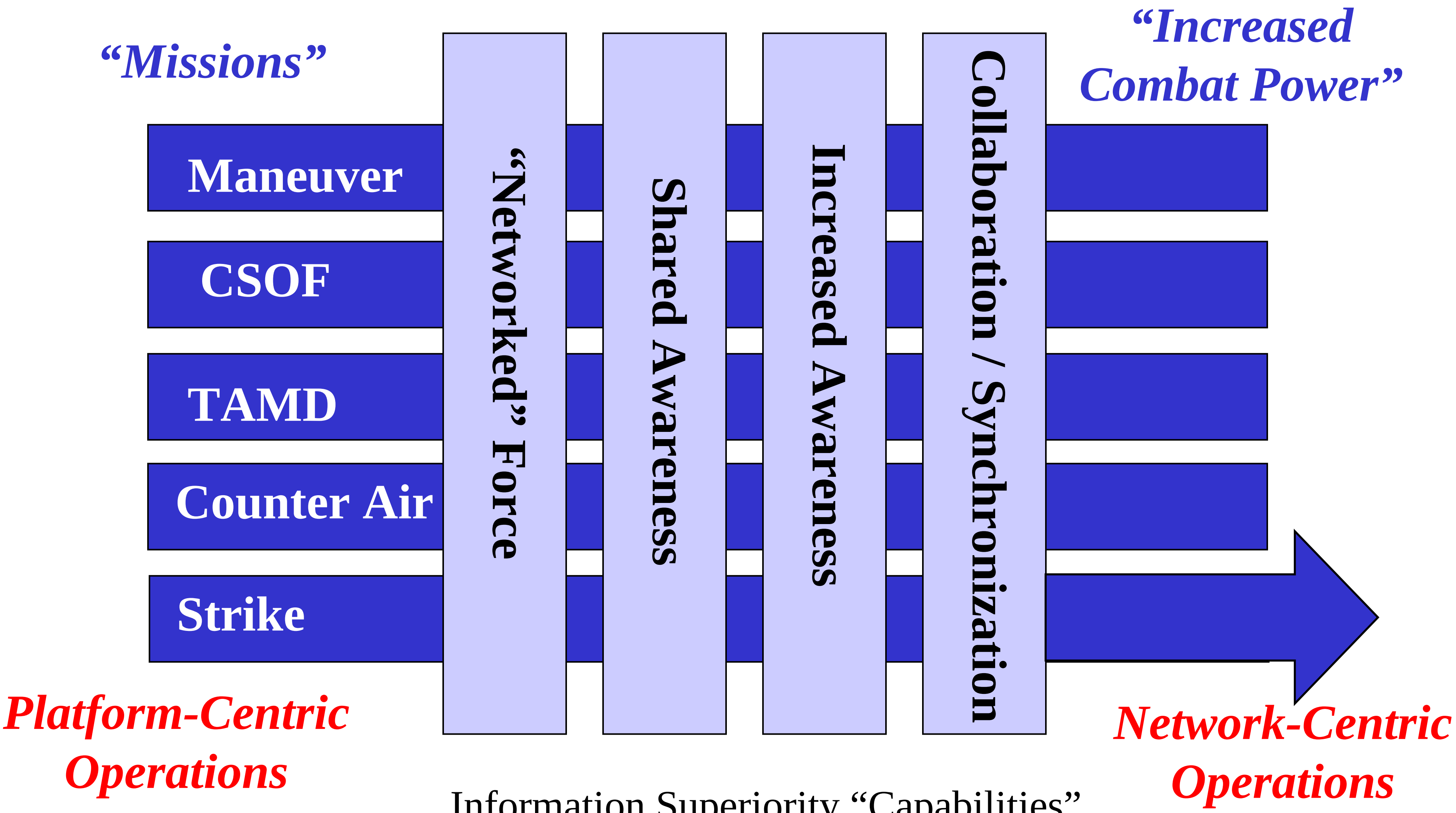
Increased Awareness
Shared Awareness

Increased Speed of Command
Effective Self-Synchronization

Increased Survivability
Streamlined Combat Support
Higher Tempo of Operations
Greater Lethality

The Power of Network-Centric Operations: Emerging Evidence

Agenda
back
more



"Missions"

Maneuver

CSOF

TAMD

Counter Air

Strike

"Networked" Force

Shared Awareness

Increased Awareness

Collaboration / Synchronization

"Increased Combat Power"

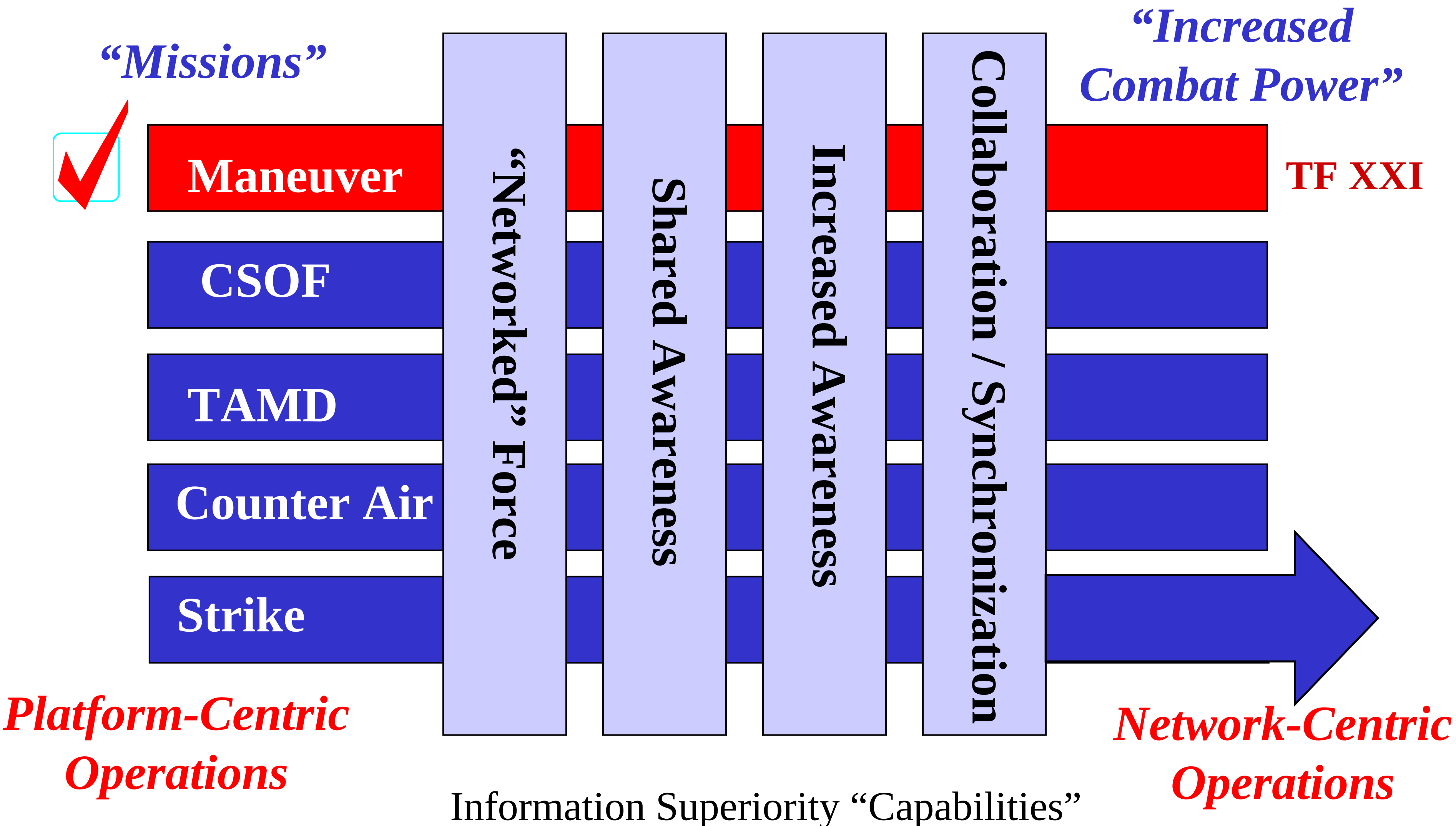
Platform-Centric Operations

Network-Centric Operations

Information Superiority "Capabilities"

The Power of Network-Centric Operations: Emerging Evidence

Agenda
back
more



"Missions"

☑ Maneuver

CSOF

TAMD

Counter Air

Strike

"Networked" Force

Shared Awareness

Increased Awareness

Collaboration / Synchronization

"Increased Combat Power"

TF XXI

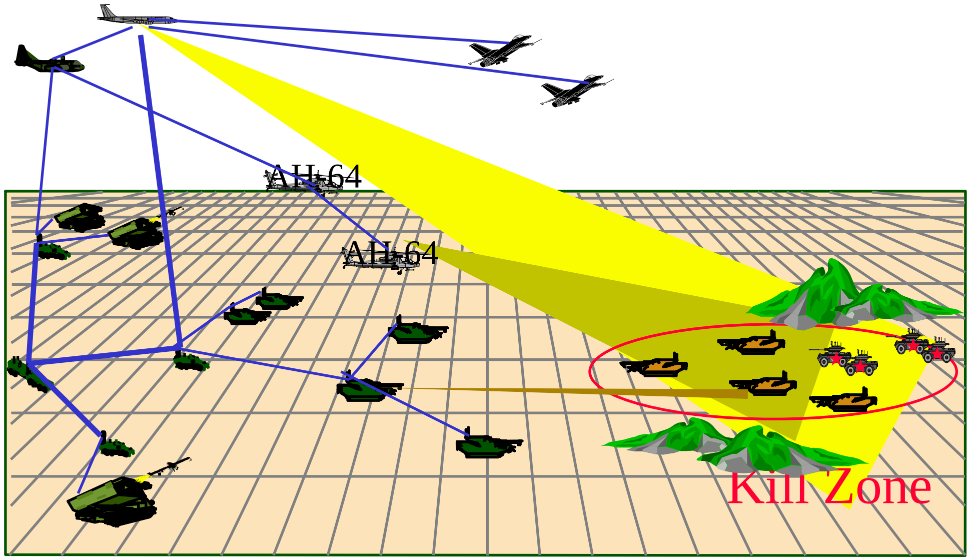
Platform-Centric Operations

Network-Centric Operations

Information Superiority "Capabilities"

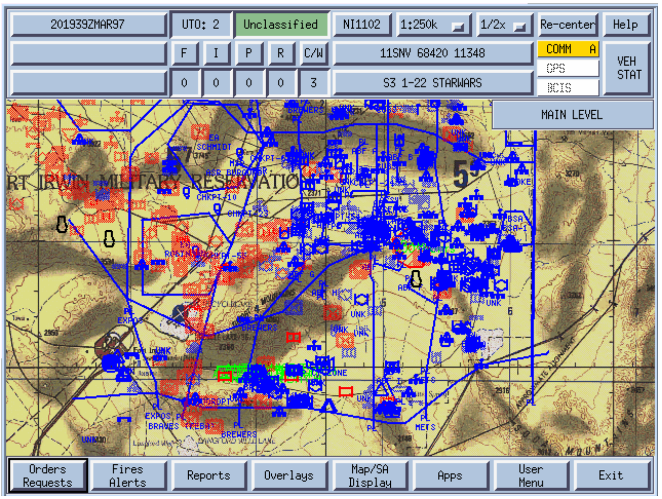
Agenda
back
more

Task Force XXI AWE



Shared Battlespace Awareness

- **Where Am I?**
- **Where Are My Buddies?**
- **Where Is the Enemy?**



Task Force XXI AWE

Agenda
back
more

	Before/After	OPTEMPO	Lethality	Survivability
• Plan Development (Div)	72 vs 12 hrs.	■		
• Call for Fire	3 vs 0.5 min		■	
• Deliberate Attack (Co)	40 vs 20 min	■	■	■
• Hasty Attack (Co)*	.49:1 vs 1.24:1 (2.5x)	■	■	
• Defense in Sector*	Loss vs Win (2.5x)		■	■
• Movement to Contact*	1.10:1 vs 1.65:1 (1.5x)		■	■

Source: Army Digitization overview -
BG William L. Bond, 20 May 98

The Bottom Line is: The EXFOR Division killed over *twice* the enemy in *half* the time, over *three times* the Battlespace, with *25% fewer* Combat Platforms using Information Age Technology

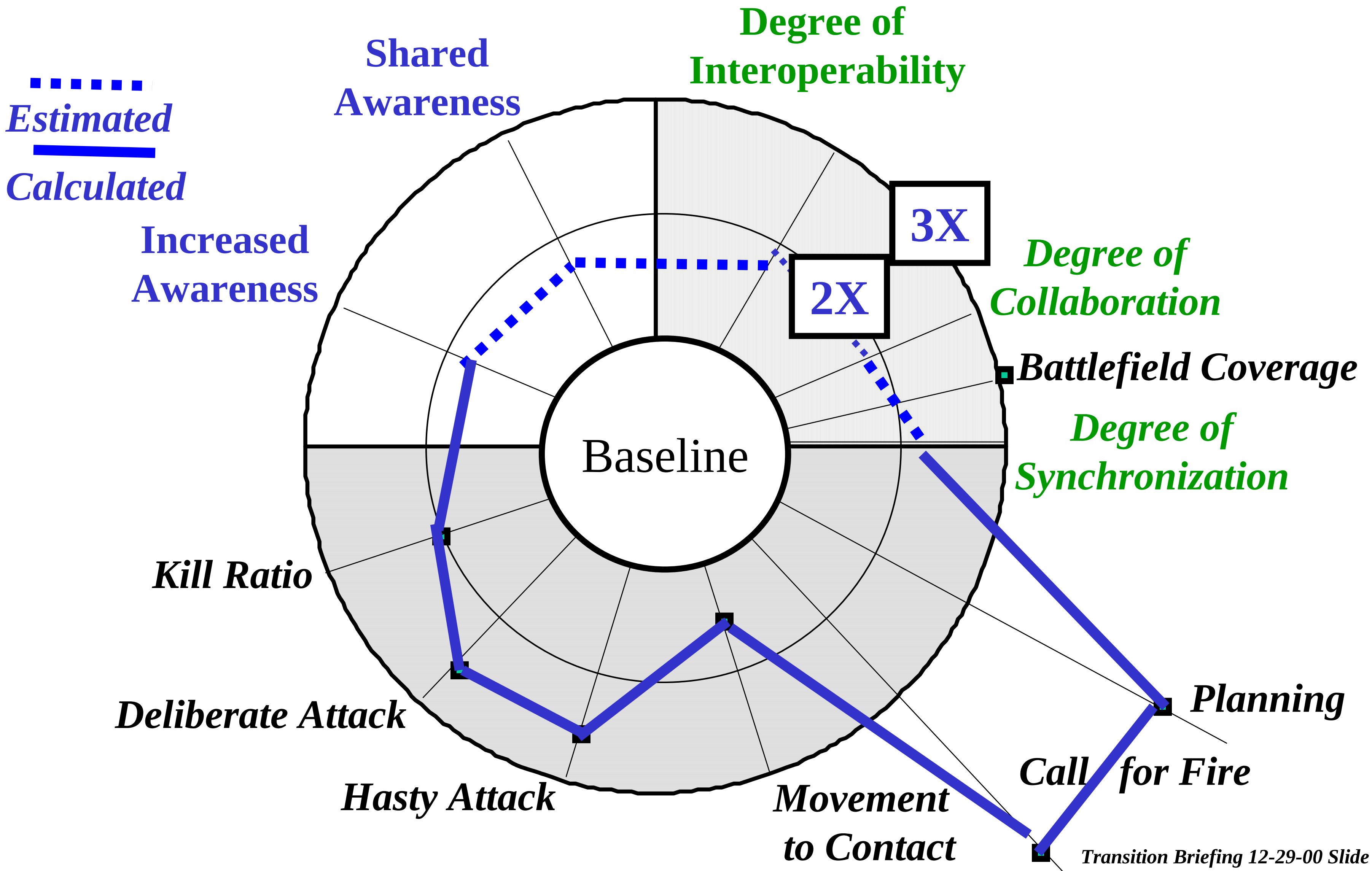
Source: Military CIS '98 - BG William L. Bond, 20 April 1998

* Task Force XXI AWE Integrated Report:
Post-NTC Modeling of Opportunities

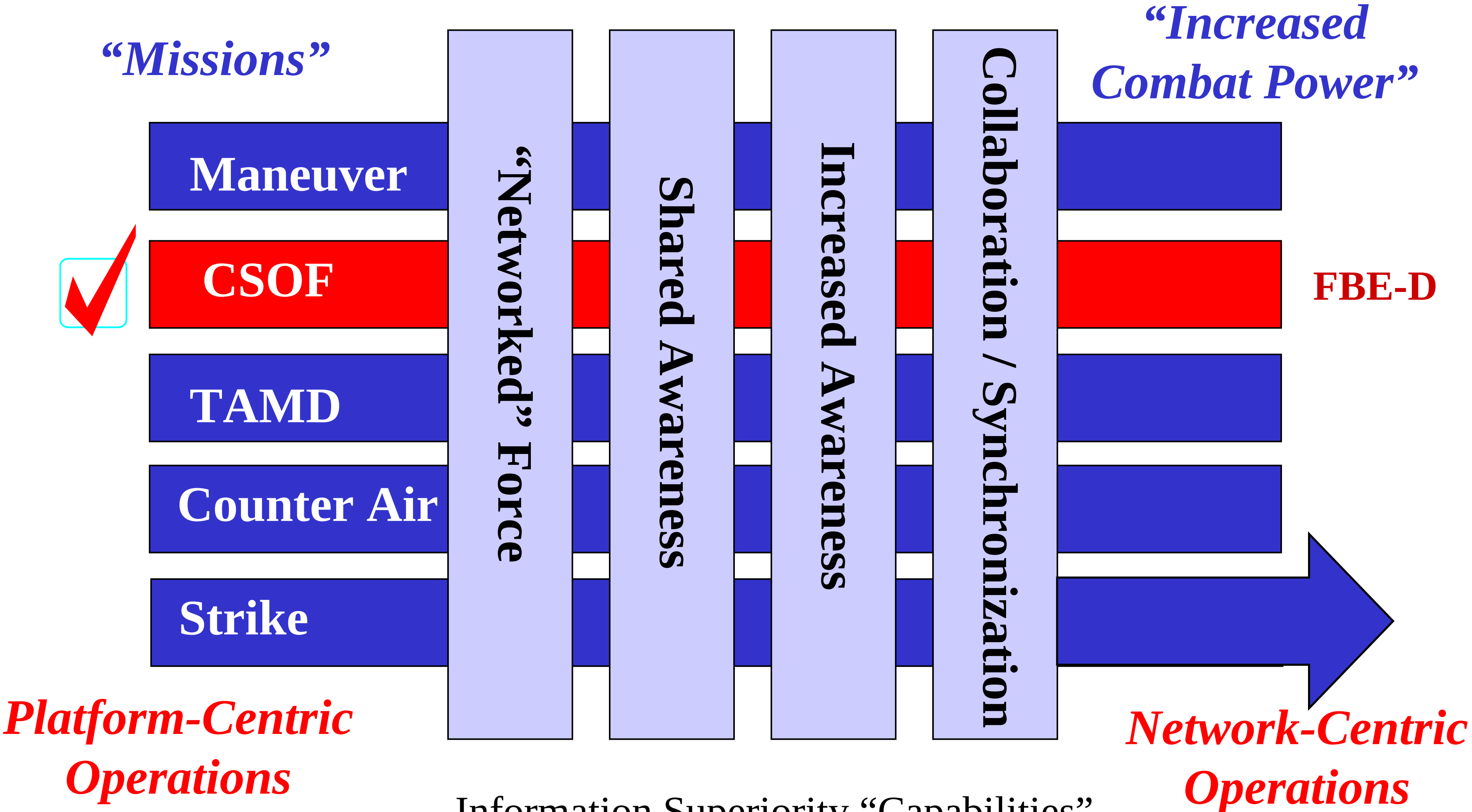
Task Force XXI

Agenda

back more



The Power of Network-Centric Operations: Emerging Evidence



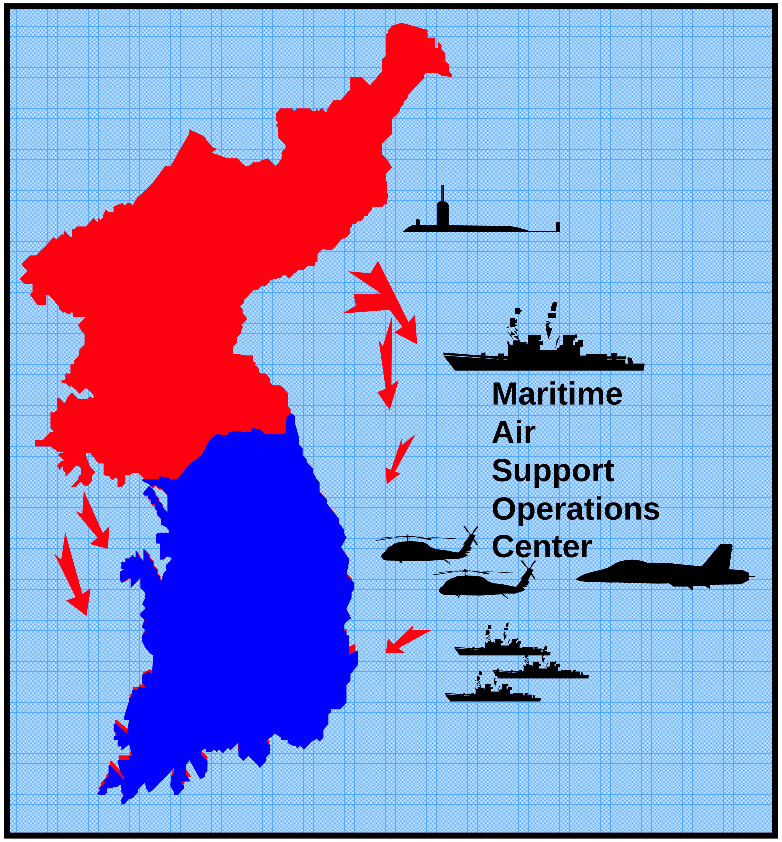
Information Superiority "Capabilities"

Counter Special Ops Forces Mission

Network-Centric Warfighting Concept:

- Land - Sea engagement network
  - Shared awareness
  - Increased engagements
- Efficient resource allocation
  - Weapon-target pairing
  - Self synchronization
- Multi-service solution
  - Coordination at “the seams”

Navy Component Commander’s Number One Problem



Source: NWDC Briefing to DRB for RMA Oversight - 14 Jan 99
Fleet Battle Experiment Delta Quick Look Report

FBE Delta Results: CSOF

Agenda
back
more

	Before/After	Self Synchronization	OPTEMPO	Lethality
• Avg Decision Cycle	43 vs. 23 min	■	■	
• Mission Timeline	50% Decrease	■	■	
• Shooter Effectiveness	50% Increase	■		■
• Assets Scrambled	15% Decrease	■	■	
• Leakers	10x Decrease	■		■

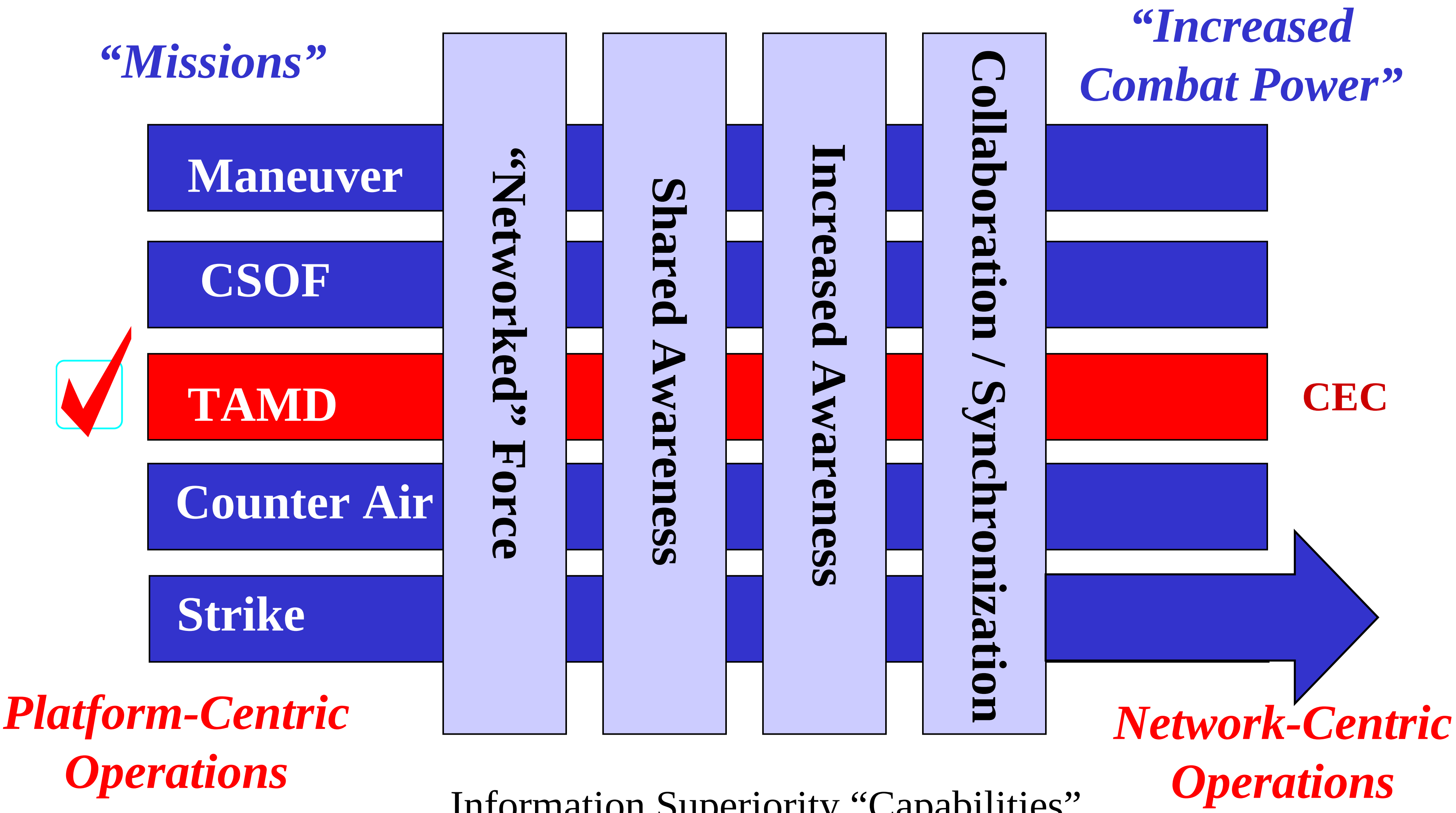
The Bottom Line: FBE Delta demonstrated the potential for a networked force provided with *shared awareness* to *self-synchronize* and to accomplish the CSOF mission in *half* the time and to reduce SOF leakers by an *order of magnitude*.

Source: Fleet Battle Experiment Delta Quick Look Report
An Assessment of IT-21 Warfighting Value-Added, 1 Mar 99

The Power of Network-Centric Operations: Emerging Evidence

Agenda

back more



Theater Air and Missile Defense

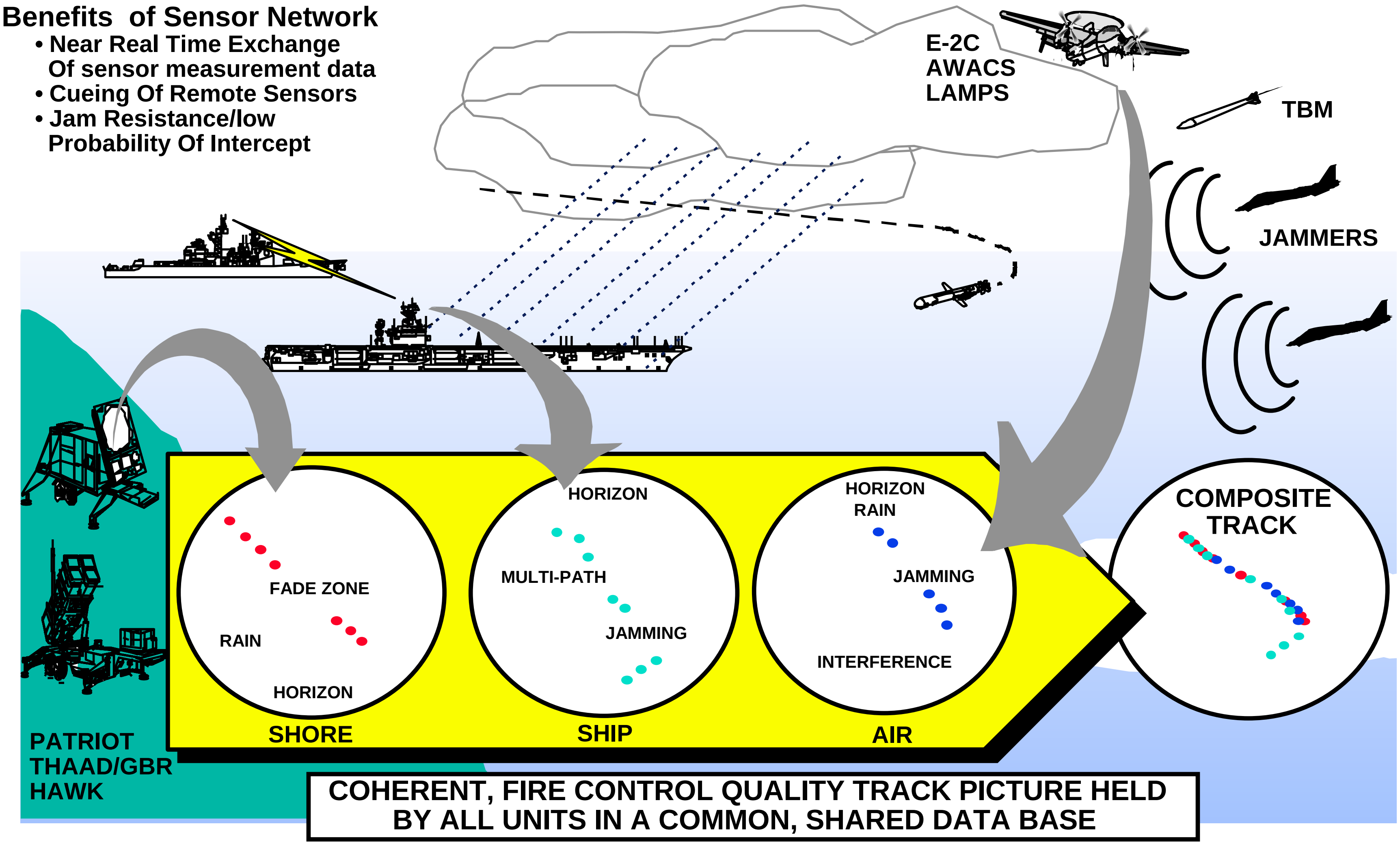
Agenda

back

more

Benefits of Sensor Network

- Near Real Time Exchange Of sensor measurement data
- Cueing Of Remote Sensors
- Jam Resistance/low Probability Of Intercept



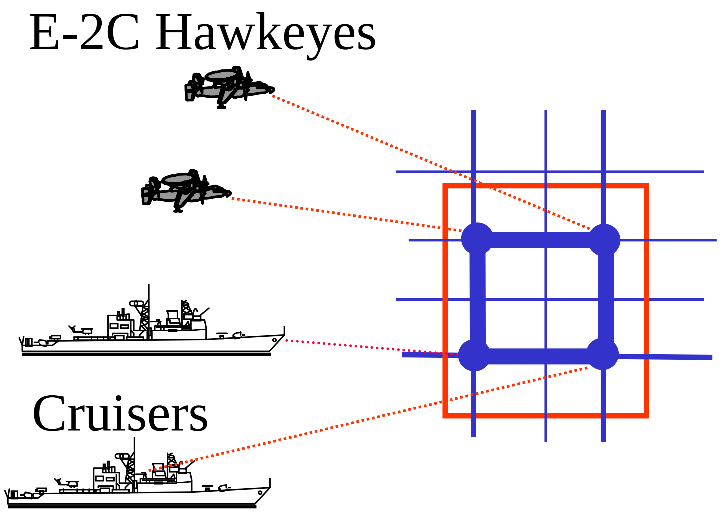
COHERENT, FIRE CONTROL QUALITY TRACK PICTURE HELD BY ALL UNITS IN A COMMON, SHARED DATA BASE

TAMD Results

Agenda

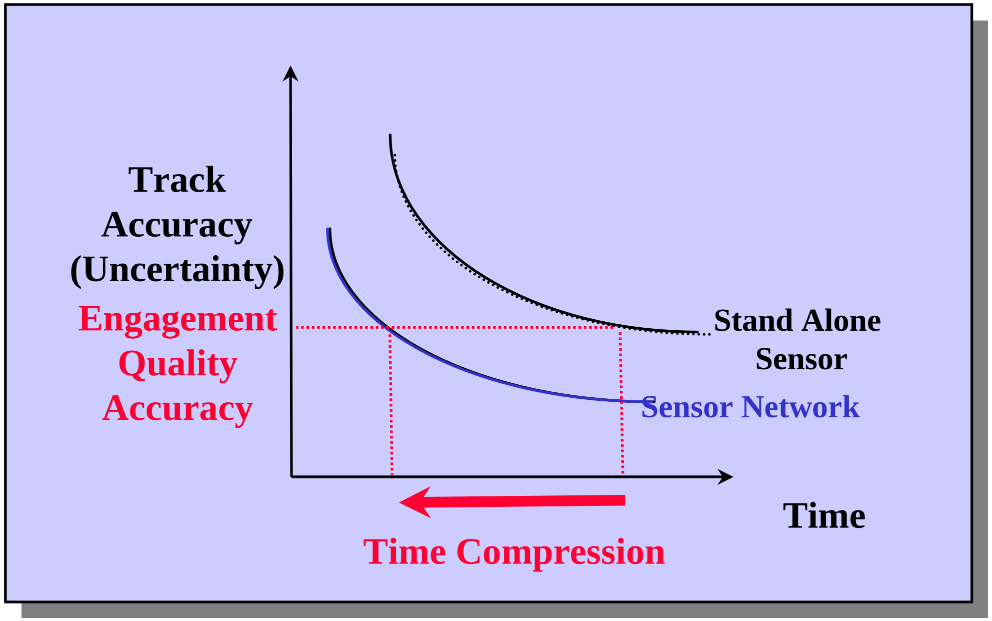
back more

Cooperative Engagement Capability



- Generates *engagement quality* Battlespace Awareness with reduced timelines
- Fuses multi-sensor data
- Quantum improvement in track accuracy, continuity, and target identification
- Extends detection ranges

Sensor Data Fusion Decreases ***Time*** Required to Generate Engagement Quality Awareness

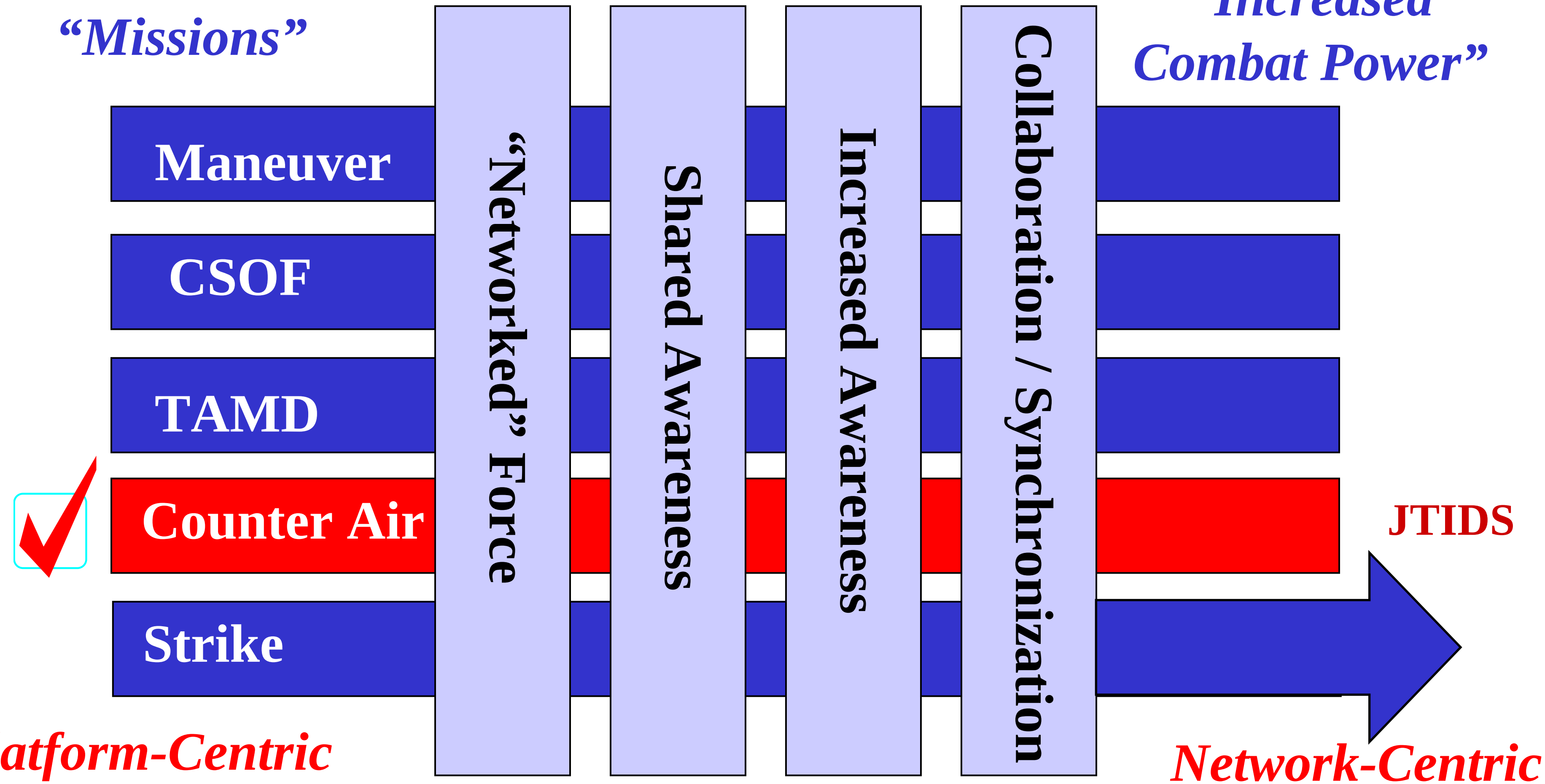


The Power of Network-Centric Operations: Emerging Evidence

Agenda
back
more

"Missions"

"Increased Combat Power"



Maneuver

CSOF

TAMD

☑ Counter Air

Strike

"Networked" Force

Shared Awareness

Increased Awareness

Collaboration / Synchronization

JTIDS

Platform-Centric Operations

Network-Centric Operations

Information Superiority "Capabilities"

Counter Air Ops w/ TDL

Agenda

back

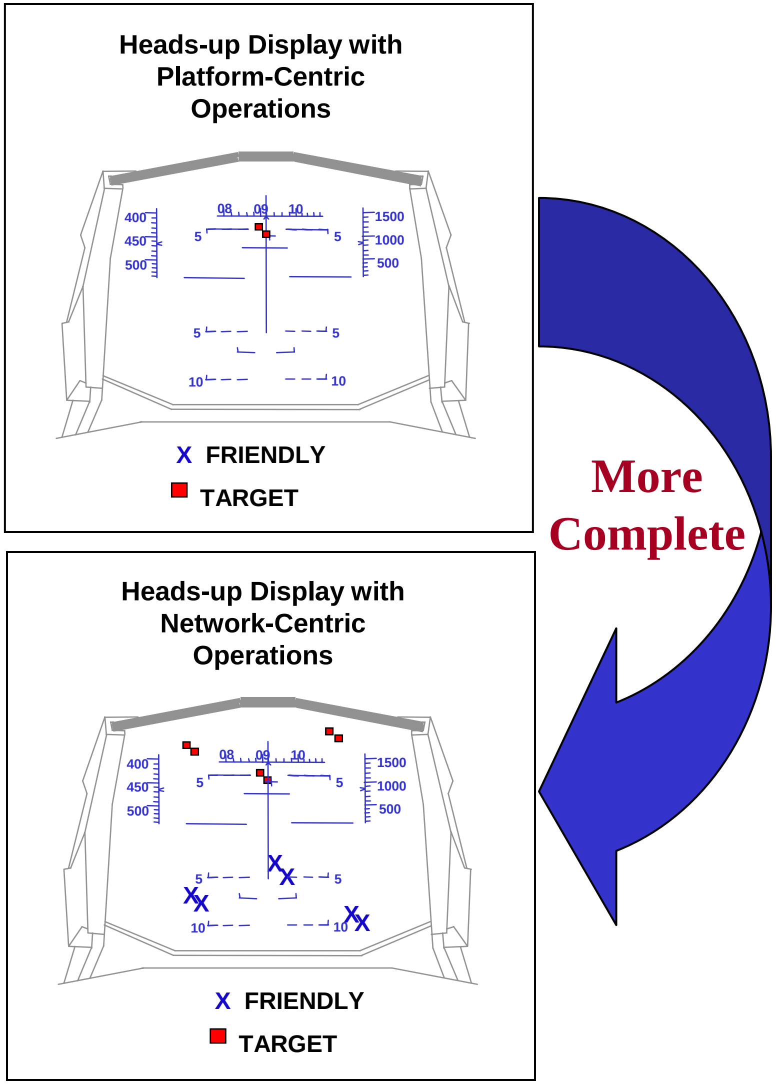
more

- Timeliness
- Accuracy
- Precision
- Relevance

✓ Completeness *

- Degree of Ambiguity / Entropy
- Availability

* Based on Critical Info Needs



Heads-up Display with Platform-Centric Operations

X FRIENDLY

🟥 TARGET

More Complete

Heads-up Display with Network-Centric Operations

X FRIENDLY

🟥 TARGET

Counter Air Results

Agenda
back
more

F15-C Air Ops: Active Missile Counter Tactics

	Without JTIDS/With JTIDS
• **Information Advantage**	**Voice Only vs. Shared Tactical Picture**
• **OODA Loop**	**Baseline Compressed with Self-Synchronization**
• **Kill Ratio**	**Night[1] 3.62:1 vs. 9.40:1 (*2.59 x increase*)** **Day[2] 3.10:1 vs. 8.11:1 (*2.61 x increase*)**

Bottom Line: JTIDS Operational Special Project demonstrated networked air crews fighting with *shared awareness* could increase combat power by over *100 %*

Source: JTIDS Operational Special Project - Report to Congress, Dec 97

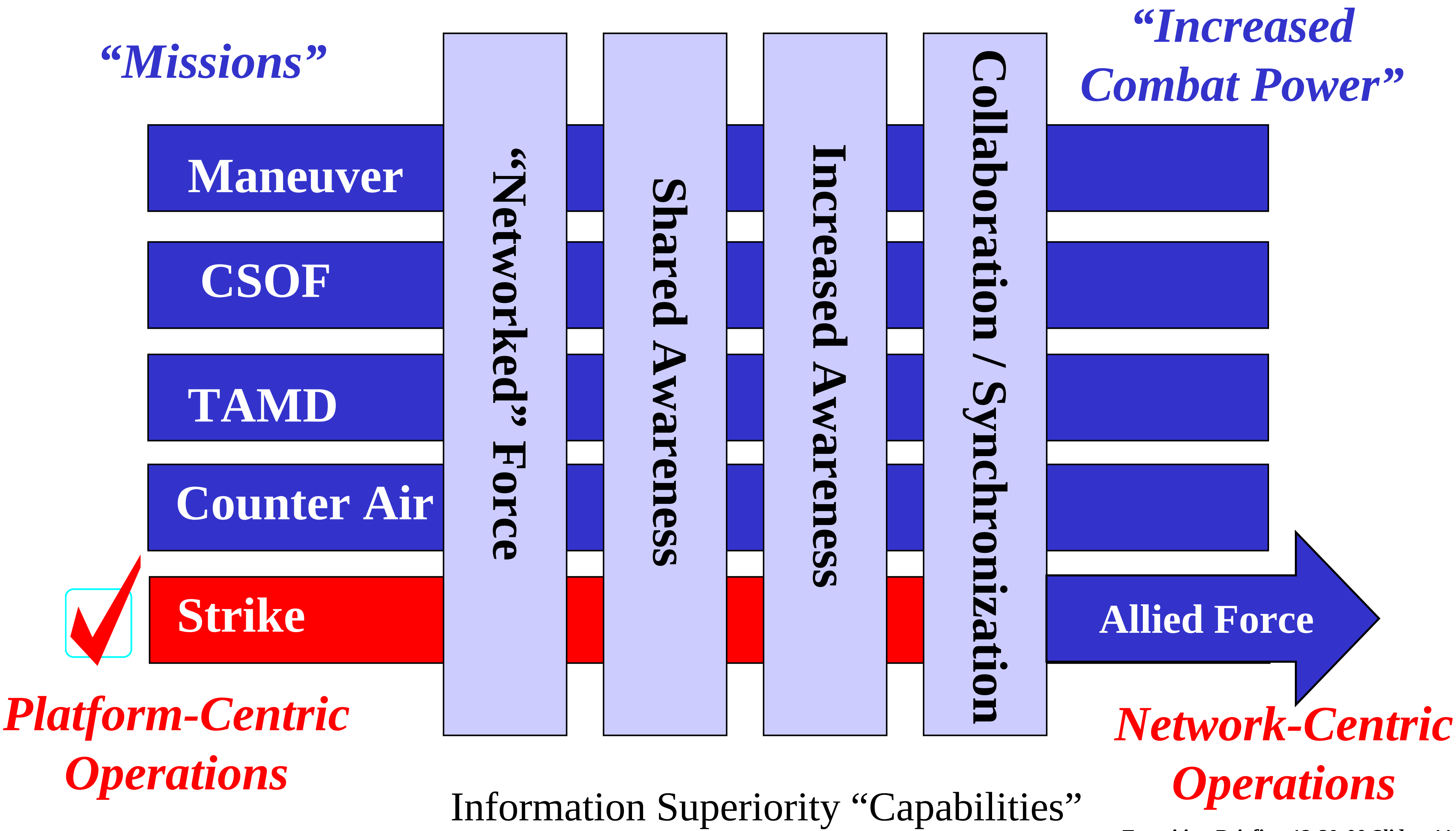
1 Active Mission Counter Tactics Fall 1996 2 Night Composite Force Tactics Spring 1997

The Power of Network-Centric Operations: Emerging Evidence

Agenda

back

more



“Missions”

Maneuver

CSOF

TAMD

Counter Air

Strike

Platform-Centric Operations

“Networked” Force

Shared Awareness

Increased Awareness

Collaboration / Synchronization

“Increased Combat Power”

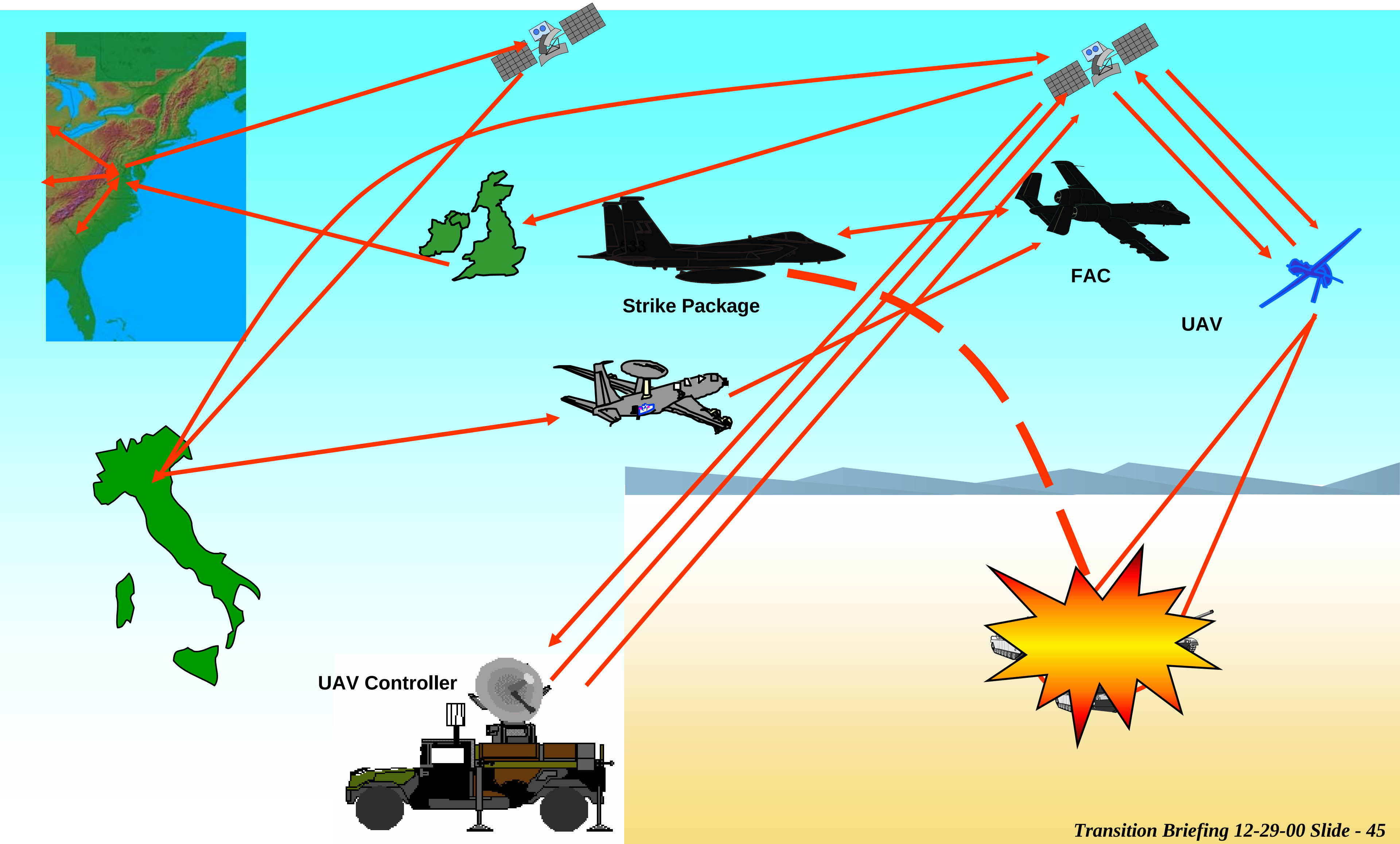
Allied Force

Network-Centric Operations

Information Superiority “Capabilities”

Networking the Kill Chain

Agenda
back
more



Strike Results

Agenda
back
more

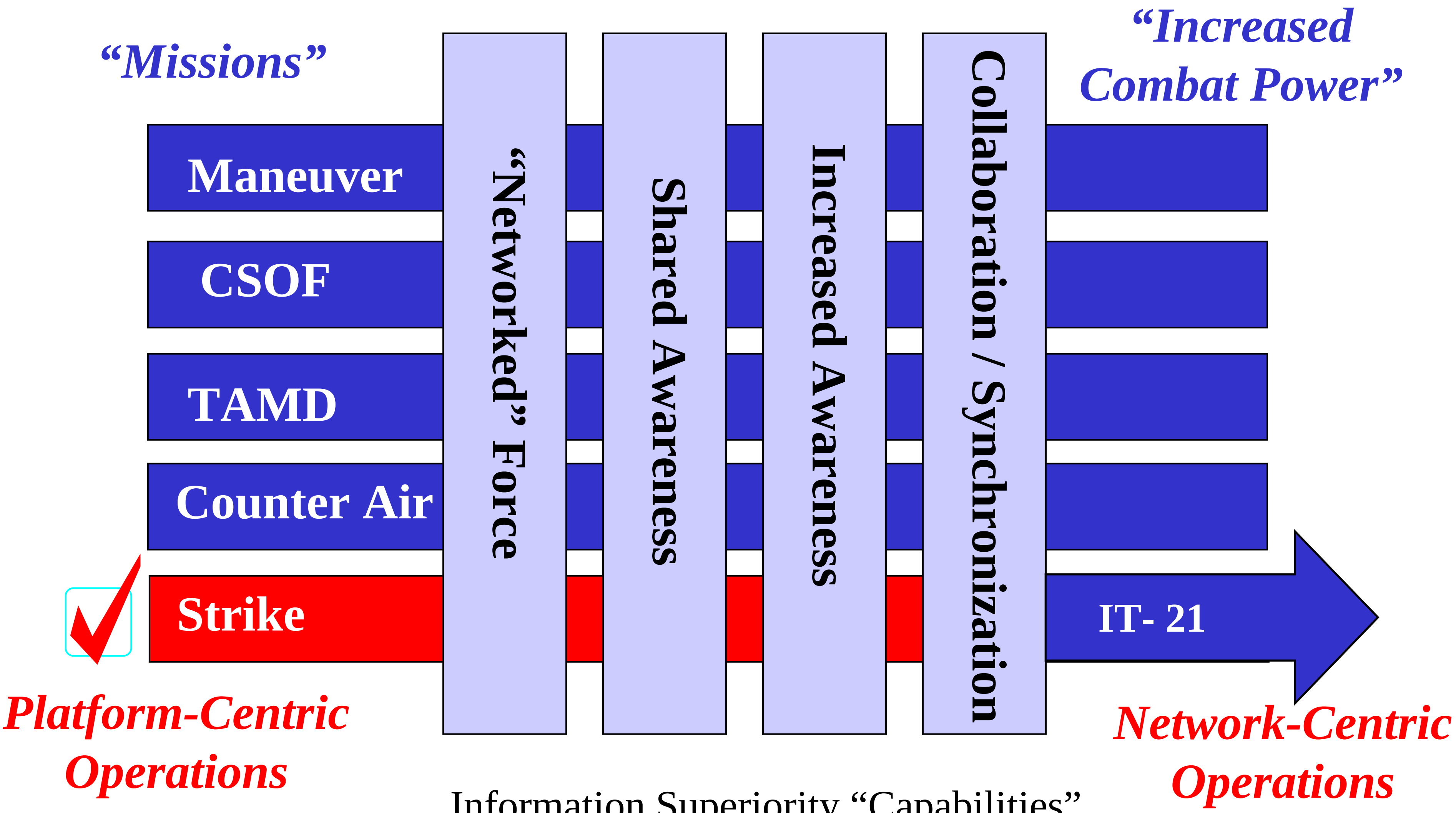
Allowed us to strike a set of targets we could not otherwise strike

The Power of Network-Centric Operations: Emerging Evidence

Agenda

back

more



"Missions"

Maneuver

CSOF

TAMD

Counter Air

☑ Strike

Platform-Centric Operations

"Networked" Force

Shared Awareness

Increased Awareness

Collaboration / Synchronization

Information Superiority "Capabilities"

"Increased Combat Power"

IT- 21

Network-Centric Operations

IT-21 Strike

Agenda
back
more

Strike Planning

- Webpage access to latest ATO, intentions message, OPTASKS, OPGENS, etc.
- IT-21 provided strike planning with new paradigm that has substantially changed the way we do business
  - Enhanced Situation Awareness
  - On-the-Fly ATO

IT-21 Strike Results

Agenda
back
more

Operational Impacts

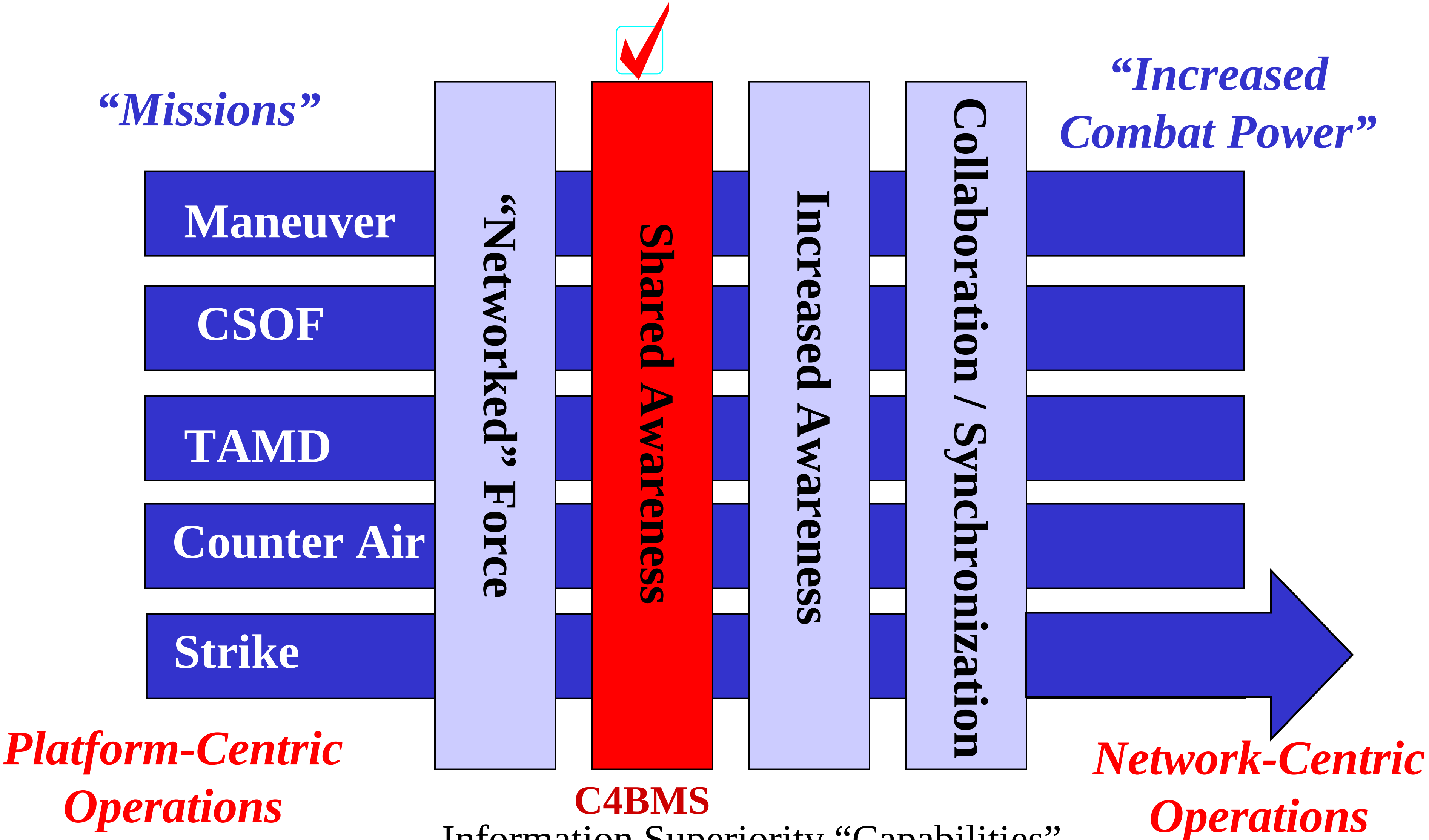
(compared to before IT-21 Baseline)

- **Objective Achieved in 34 v. 64 hrs**
- **More Kills (36%)**
- **Fewer Blue Losses (46%)**
- **More High-Priority Kills (50%)**
- **Increased Speed of Command (53%)**

* Source: Naval Simulation System (NSS)
An Assessment of IT-21 Warfighting Value-Added
prepared for ADM Clemins, 5 January 1999

The Power of Network-Centric Operations: Emerging Evidence

Agenda
back
more



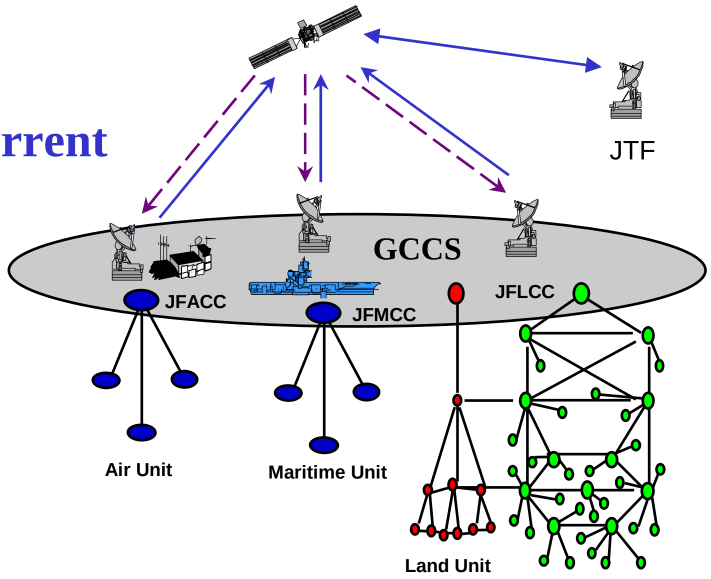
Information Superiority "Capabilities"

JTF COP

Agenda
back
more

- A Timely Joint COP & CTP With a Fused Picture of Friendly and Enemy forces is Needed for Improved Coordination and Synchronization.

Current

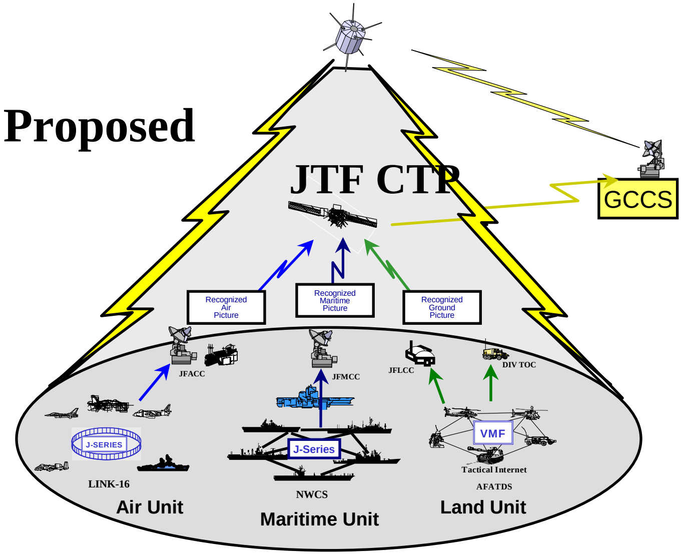


Service Roll-up - Manual Selective Blue/Red Input - Selective Roll-down Dissemination

- Separate Management, Links, Formats, and Receivers
- Inefficient Use of Bandwidth
- Burden on user to filter and correlate

Delays Often Too Long for Effective Joint Engagement

Proposed



Service Roll-up - Joint Fused - JTF CTP Broadcast Dissemination

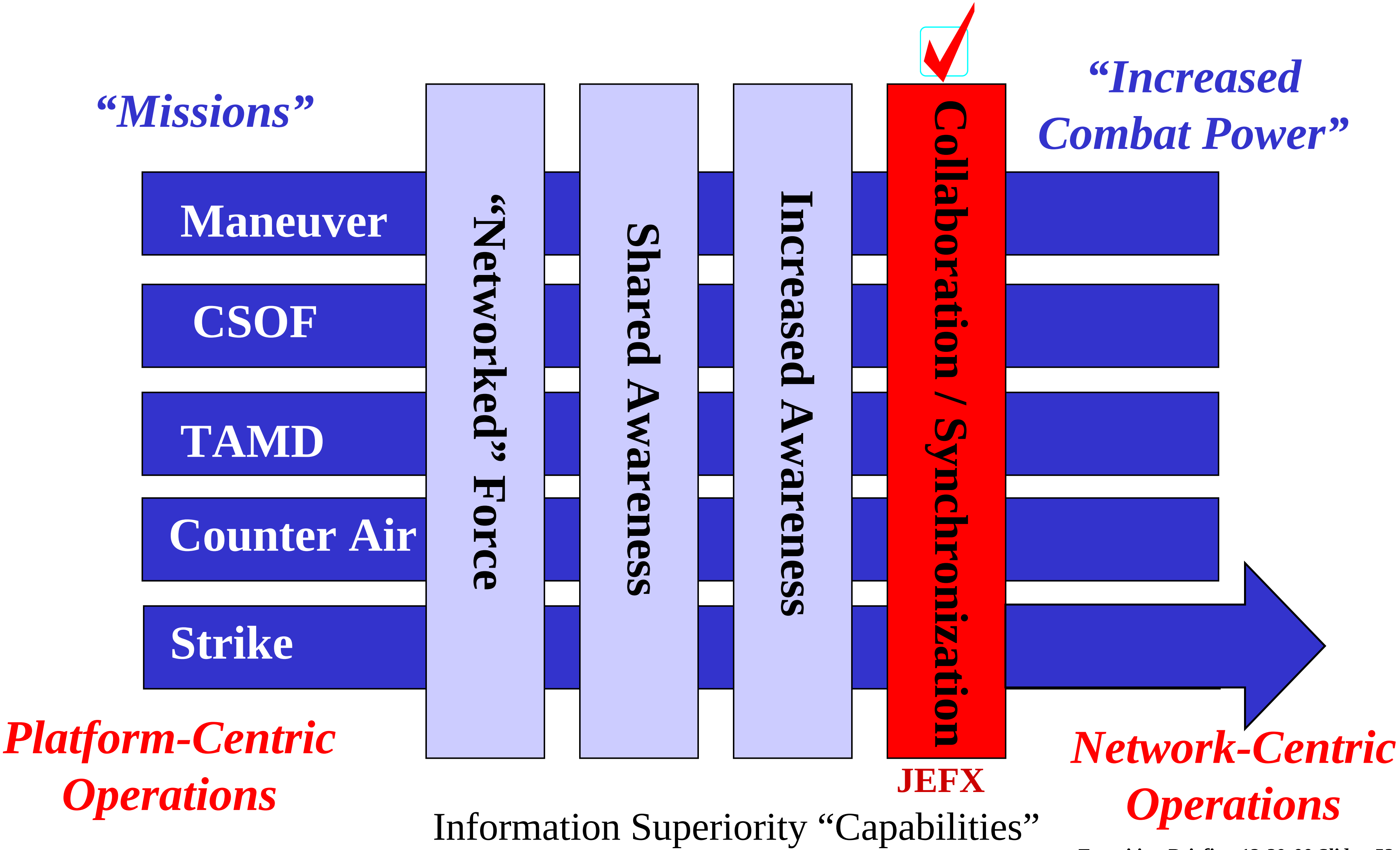
COP Results

Agenda
back
more

	Improvements
High Priority Kills	35% (1.5 : 1)
Speed of Command	50% (2 :1)
Loss Ratio (Red/Blue)	20-30% (1.3 : 1)

*Sensor-to-Shooter C4 Battle Mgt Study - J6/DSC

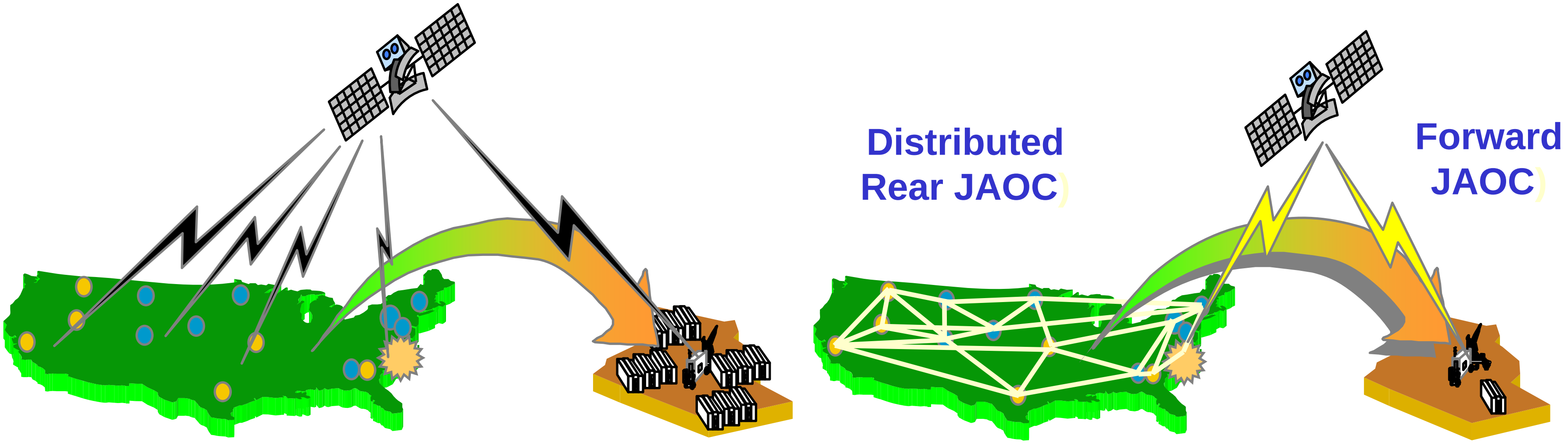
The Power of Network-Centric Operations: Emerging Evidence



Split Based Operations

Agenda
back
more

Virtual Collaboration: Moving Information - Not People



Agenda
back
more

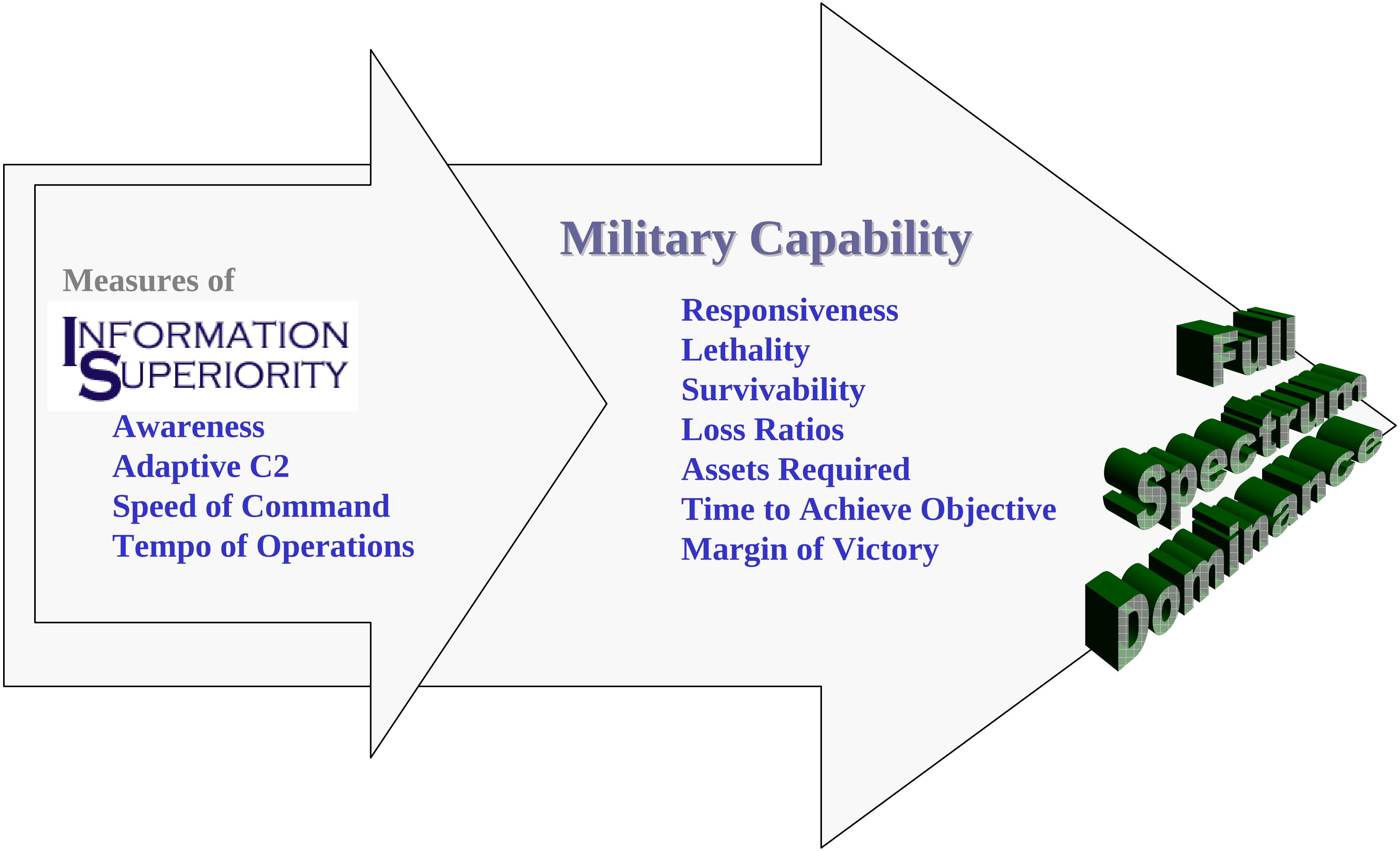
EFX ‘98 and ‘99

	Before		**After**
• **Deployed Footprint (people)**	**1500-2000**	**vs.**	**100-300**
• **Deployment Timeline**	**10-15 Days**	**vs.**	**1-2 Days**
• **Air Lift Required**	**25 C-17 Loads**	**vs.**	**2 - 3 C-17 Loads**

Source: EFX ‘98 Final Report

Agenda
back
more

Summary of the Growing Body of Evidence



Measures of

INFORMATION SUPERIORITY

- Awareness
- Adaptive C2
- Speed of Command
- Tempo of Operations

Military Capability

- Responsiveness
- Lethality
- Survivability
- Loss Ratios
- Assets Required
- Time to Achieve Objective
- Margin of Victory

Full Spectrum Dominance

Drill Downs

Network Centric Enterprise

Network Centric Enterprise

Agenda

back

Drill Downs

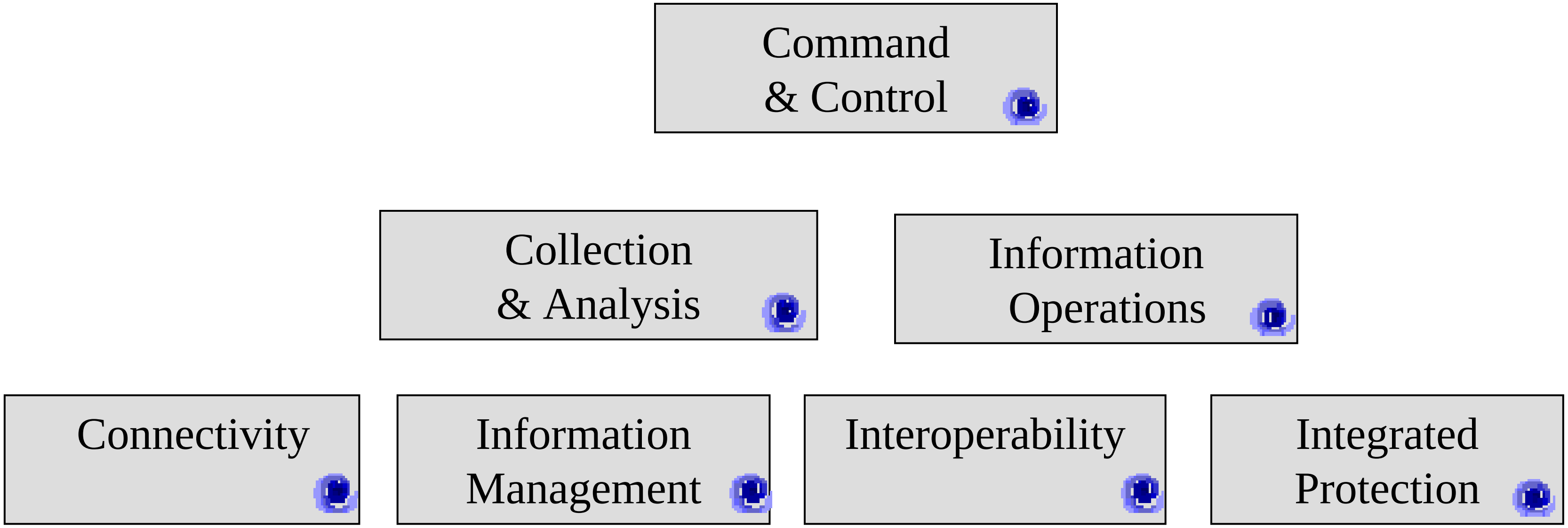
Building Blocks
of
Information Superiority

INFORMATION SUPERIORITY

Building Blocks

Agenda

back



Command & Control

Collection & Analysis

Information Operations

Connectivity

Information Management

Interoperability

Integrated Protection

Collection and Analysis: Vision

- Integrated and responsive ISR capabilities operating in a collaborative enterprise assuring delivery of timely, relevant information for the NCA and Joint/Combined forces and supported by an Infostructure/TPED capability that provides for:
  - Integration of the Operational and ISR communities
  - Integration across space, air, maritime, and terrestrial ISR systems
  - Integration of the Intelligence, Surveillance, and Reconnaissance communities
  - Interactive Collection Management across national, theater, and tactical ISR assets
  - Advanced Collectors and New Capabilities
  - Multi-INT Collaboration between HUMINT, IMINT, SIGINT and MASINT.

Collection and Analysis: Programs

Agenda
back
more

- Global Hawk
- Space-Based Infrared Radar System
- Tasking, Processing, Exploitation, & Dissemination
- Joint SIGINT Avionics Family

Collection and Analysis: Shortfalls

Agenda

back

- SIGINT
  - Lack of Signature Acquisition Against Hard Targets
    - and/or to Defeat “Denial and Deception”
  - Lack of SIGINT Against Fiber-Optics and Encrypted Signals
- High Density/Low Demand Assets
- TPED
  - Inability to Process EIS/FIA Level Imagery Collections
- Inadequate Information Capabilities to Support Time-Dynamic and Information-Intensive Operations
- No Coherent MTI: Lack of Detection, Identification, and Tracking
- Lack of Interoperability Between “INTs”
- No Beyond Line of Sight (BLOS) Comms
- Shortages of Appropriately Skilled Personnel
- Inability to Build and Share an Integrated View of the Battlespace

Low Density/High Demand (LD/HD)

Agenda

back

- Issue:
  - – no planned increases in HD/LD assets (e.g. U2, RJ)
  - – requirements expected to continue or increase
  - – no relief in the short term
    - – fixes (e.g. Global Hawk) are long term
    - – no funds available within the FYDP

Command and Control Vision

- An integrated and seamless capability to provide Joint and Coalition warfighters with: a comprehensive operational picture relevant to their needs; the tools and products to rapidly conduct mission planning at all levels; and the capability to control forces

Command and Control Programs/Initiatives

Agenda
back
more

- Global Command and Control System (GCCS) family
  - C2 system for NCA, joint Staff, combatant commands, Services, Defense agencies, joint task forces (JTFs), and components
- Family of Interoperable Operational Pictures (FIOP)
  - an integrating strategy to guide and direct other programmatic efforts with a goal of ensuring horizontal interoperability of Service C2 systems
- Single Integrated Air Picture (SIAP)
  - product of fused, common, continual, unambiguous tracks of airborne objects
- Joint Mission Planning System
  - effort to employ common mission planning information and systems
- DOD-IC Collaborative Planning Tool Strategy

Command and Control Shortfalls

Agenda

back

- Common Relevant Operational Picture (CROP) Incomplete
  - effort to provide operational pictures with only information relevant to mission being performed
  - appropriate filters and dada accessibility not available
- Integrated Mission Planning
  - resource visibility primarily by Service
  - numerous, non-interoperable collaborative tools and products
- Control of Resources at Service Level
  - equipment plus operational procedures and doctrine

Common Relevant Operational Picture

Agenda
back

- Issue: Common Relevant Operational Picture (CROP) Incomplete
- Way Ahead:
  - Integrated Air Picture (SIAP effort)
  - Integrated Ground Picture (MS C2 FOSC effort)
  - Integrated Maritime Picture (SIP effort)
  - Family of Interoperable Pictures (FIOP effort)

Information Management Vision

- Providing the Right Information to the Right Place at the Right Time in the Right Format in accordance with Commanders' Information Dissemination Policies

Information Management Programs/Initiatives

- Information Dissemination Management Program
  - – C3I IDM Framework Document Approved
  - – C3I Working Closely with CIO to Ensure IDM Linkage to GIG
  - – GIG Architecture defines Information Management and Information Distributions Services
- Integrated Broadcast Service
  - – Approved Technical Requirements Document (TRD)
  - – Completed Phase I Contract Award, Program Development Risk Reduction (PDRR) 3QFY00
  - – Fielding Joint Tactical Terminal (JTT)

Information Management Shortfalls

Agenda

back

- No Means to Dynamically Adjust the Flow of Information/Data to the Most Efficient Communications Pathway Available at the Time of Delivery.
  - Lack of Management Plans Identifying How to Address and Manage Multiple Security Domains.
  - Lack of a Single Capability Strategy to take Advantage of Broadcast, INTERNET and other Emerging Technologies.
  - Lack of Integrated Cross-Functional Capabilities to Manage Information Dissemination.
- Lack of clear policy to support content management
  - Responsibility for establishing and maintaining web liks
  - Visualization, bandwidth, and quality of service choices
  - Community of interest use of PKI technology

Communications & Spectrum Vision

Agenda

back

- **Communications:** Connectivity, bandwidth, and interoperability sufficient to enable network-centric operations

- **Spectrum:** To maintain assured access to the electromagnetic spectrum resource required to successfully accomplish national security and military objectives (enable JV2020) and to effectively and efficiently use this finite resource.

Communications Programs/Initiatives

- SATCOM modernization
  - Advanced EHF
  - Wideband Gapfiller/Advanced Wideband
  - Advanced Narrowband
  - Global Broadcast Service
  - Teleport
- Joint Tactical Radio System
- Defense Messaging System
- DISN Enhancement Program (DEP)

Communications Shortfalls

Agenda

back

- Insufficient beyond-line-of-sight bandwidth
- Interoperability problems
- Joint tactical data/voice capability not fully deployed by 2010
- Insufficient Quality of Service to support distributed computing operations

Spectrum Initiatives

Agenda
back
more

- Implementation of Omnibus Budget Reconciliation Act ‘93 and Balanced Budget Act ‘97
- Enforce / redefine frequency acquisition process
- Common costing/analysis model
- Impact public safety wireless advisory committee
- Define Joint Warfighter spectrum requirements and pursue doctrinal/process technical improvements
- Update DoD Spectrum policy/strategic plan

Spectrum Challenges

Agenda

back

- International Mobile Telecommunications (IMT)-2000
- Ultra Wide Band Threat to Global Positioning System
- Notice of Proposed Rule Makings
  - National Telecommunications and Information Administration (NTIA) Cost Reimbursement
  - Federal Communications Commission (27 MHz)
- World Radio communication Conference 2003
- Joint Tactical Information Distribution System
- (JTIDS)/Universal Access Transceiver (UAT)

Space Policy & Space Systems Vision

- **Space Policy:** Formulate, coordinate, and oversee implementation of U.S. Government and DoD policy guidance for the conduct of space and related activities to facilitate transformation and provide the space power and information superiority necessary to achieve U.S. national security objectives
- **Space Systems:** To ensure DoD, civilian and commercial requirements for access, space control, navigation, launch, satellite operations and weather are prioritized, coordinated and operationalized in order to fully exploit the benefits of operating in space.

Space Policy Programs/Initiatives

Agenda
back
more

- Management and organization
  - SecDef response to Space Commission’s recommendations
  - Implementation of SecDef adopted NRO and NIMA Commission recommendations
- DoD policy and guidance
  - SAP/SAR policy
  - DoD Directive on DoD Support to Commercial Space Activities
  - Mir reentry contingency operations plan
- Space control
  - Operation Noble Anvil Lessons Learned
  - Space Control Security Classification Guide
  - Review of DoD Policy on Space System Protection
- Remote sensing
  - Private remote sensing space system operating licenses / DoD-IC next generation remote sensing assessment
  - Report to Congress on Military Utility of Commercial Imagery
- International cooperation
  - Exercise of Host Nation Notification Procedures
  - Space cooperation with UK, Canada, Australia, Italy, Spain, Germany, etc.
- Arms control and related activities
  - United Nations’ Conference on Disarmament / Committee on Peaceful Uses of Outer Space
  - Missile / space launch nonproliferation agreements

Agenda

back

Space Policy
New Initiatives

- Implementation of SecDef adopted Space, NRO, and NIMA Commission recommendations
- Interagency review of Presidential directives regarding space and related activities
  - National Space Policy, Space Transportation, Foreign Access to Remote Sensing Space Capabilities, Nonproliferation and Export Controls, GPS, etc.
- Review of DoD Directives and Instructions on space and related activities
  - DoD Space Policy, Space Support, Space Force Enhancement, Space Control, Space Force Application, Laser Illumination of Space Objects, etc.
- Review of DoD policy guidance regarding space control testing
- Review of DoD policy guidance regarding space weapons
- Space control-information operations integration
- Remote sensing grand strategy
- Space arms control countervailing strategy
- International defense space cooperation strategy

Space Systems Programs/Initiatives

Agenda

back

more

- Space Control Broad Area Review
  - Space Surveillance Modernization
  - Lead Service Systems Integrator for Space Surveillance
  - Space Control Test Range
  - Improved Space Denial Capability
- EELV: Competitive launch capability at reduced cost
- GPS
  - Modernization from IIF to IIR to GPS III
  - Equip platforms with new User Equipment (UE)
- NPOESS
- KE ASAT: Release of funds to complete program

Space Systems Shortfalls

Agenda

back

- Spectrum Conflicts
  - Moving to USB for Satellite Control
  - Protecting GPS’s Fragile Spectrum
- Money for Expensive Space Programs
  - Modernizing Space Surveillance System
  - Investing in the Development of Space Denial Systems
  - Commitment of Funds for Environmental Sensing
- Prevention and Protection Concerns
  - Achieving Cost-Effective Protection of Space Systems
  - Immediate Need for GPS NAVWAR and Anti-jam Features
- Technology Hurdles
  - Decrease the Cost of Space Launch
  - Enhance Capability of Developmental Denial Systems

Agenda
back

Space Surveillance Modernization

the way ahead

- The goal: Modernize Space Surveillance Network
  - achieve improved space situational awareness
  - be the sole space surveillance info provider to commercial and foreign entities
- The long term plan (attempt in ‘03 APOM):
  - $127M over the FYDP
  - buy GEODDS spares, full C2 upgrades, add small aperture telescopes, improve Cobra Dane
- Short term compromise
  - $5M, $5M, $1M ($9M total) in ‘01, ‘02, ‘03
  - $9M for GEODDS spares
  - $2M to begin C2 upgrades

Integration Vision

- To ensure the Commander can direct his full energies to fighting the enemy vice fighting with his non-integrated and non-interoperable C4ISR systems
  - CJTF capabilities are integrated and operational upon entry into the assigned area
  - Information flow is assured among all levels of command and battle management
  - Sustainment of information technology will not impede operational flexibility

Integration Initiatives

Agenda
back
more

- C4I Support Plan review and issue resolution
  - DoD-wide review and issue resolution of newly acquired weapon and C4ISR systems for interoperability and supportability req'ts
- Information Superiority Investment Strategy
  - An across the board examination of DoD missions for information shortfalls, alternative investment options, and offset proposals
- Acquisition
  - Evolutionary/incremental acquisition, system of systems oversight, interoperability assurance
- Interoperability
  - Joint Command and Control Integ and Interop Group
  - Joint Defense Engineering Plant
  - JFCOM as Jt Forces Integrator
- GIG Integrated Architecture
  - Operational, system, and technical views provide integrated CJTF perspective
  - Joint Information Exchange Requirements lnked to Joint Staff's Joint Operational Architecture

Integration Shortfalls

- The Department is organization and system centric vice information and mission centric
- Title 10 allows/promotes independent non-joint acquisitions
- System-of-system/portfolio mgmt and oversight is limited to a small set of programs
- Determination of the required levels of interoperability and subsequent measurement of the value in terms of outcome-base metrics are not defined
- Resourcing for interoperability solutions for legacy systems is minimal,
- Acquisition reform philosophy perceived to be in conflict with improving interoperability (standards),
- The use of architecture as a general tool for integrated is not yet widely accepted

Intelligence Shortfalls: Workforce

Agenda

back more

- Skilled people are foundation for successful intelligence support
- Critical shortfalls in linguists, all-source analysis, HUMINT, MASINT, S&T, imagery, targeting, and IO
  - Also lack appropriate analytic, management, & training tools
- Adversely impacts all intelligence support of National Security Strategy missions
- Workforce composition, training, skills and tools must be guided to meet changing work environment
  - Focus on skill areas requiring years of experience to reach full capability
- New business practices, privatization, technological opportunities, & pressures for extraordinary breadth of coverage will shift traditional tasks to commercial, academic, & other non-government activities

References: Defense Intelligence for the 21st Century (DI-21), NSA Transformation Plan, OASD(C3I) HUMINT Study, DIA Four Thrusts Initiative, Congressional Report Language

Intelligence Shortfalls: Policy/Process

Agenda
back
more

- Need balanced, integrated requirements prioritization process
  - Limited Intelligence Community resources & competing requirements
  - Some progress -- IC Multi-Int Architecture Plan
  - "National" versus "Tactical" requirements debate obscures issues and hinders resolution
- Congressional & DoD stakeholders seek transitioning single discipline Tasking, Processing, Exploitation, & Dissemination (TPED) approaches to integrated, Multi-Int TPED process
  - TPED is "Number 1" ISR shortfall
  - Need to realize operational & fiscal efficiencies
  - Require process modeling, benefits assessment, roadmap, & investment strategy
- Inadequate dissemination of intelligence in a Coalition Environment
  - Integration of coalition partners key to IS
  - Intelligence must be part of portrayal of the battlespace
  - IT/interoperability challenges can be overcome
  - National disclosure policy/release procedures have not kept pace
- Lack of policy on multi-level security, storage & dissemination

References: Defense Intelligence for the 21st Century, Congressional Report Language, Kosovo Lessons Learned

Intelligence Shortfalls: Technology/Material

Agenda
back
more

- Information Operations increases demand for analytic detail & specificity
- Considerably more effort required for collection & analysis of foreign cyber & physical infrastructures and critical nodes
  - Collection & processing tools for level of technical data
  - Integrated databases for network reconstruction
- SIGINT and MASINT capabilities need to meet emerging challenges
  - R&D and investment in new collection & processing technologies
  - Support Information Operations
  - Counter transnational & asymmetric threats -- terrorism, weapons/technology proliferation, & weapons of mass destruction
  - Defeat denial & deception (e.g. hardened deeply buried targets)

References: CyberWarfare National Intelligence Estimate, Defense Intelligence for the 21st Century, NSA Transformation Plan, MASINT Independent Program Evaluation, Congressional Report Language

What Needs to Be Done:
Intelligence

Agenda

back

- Emphasize developing & preserving the high value, long lead-time capabilities of the DoD IC. Areas of focus:
  - Highly specialized personnel and change agents
  - Collection capabilities against emerging technologies
  - Processing, exploitation and analytic tools requiring extensive development
- In context with above imperatives, ASD(C3I) will
  - Postulate solutions for recruiting, equipping, training & retaining critically needed intelligence specialists
  - Present solutions to obstacles inherent in current policies & procedures
  - Identify means of enhancing DoD IC physical & cyber infrastructures and making interoperability & integration an operational reality
  - Look for methods to institutionalize intelligence support to IO
  - Ascertain where policy and resources are deficient in allowing US and coalition partners to work from a common operating picture
  - Consider use of Knowledge Management systems & other "smart tools" to increase effectiveness of existing and projected intelligence assets

Integrated Protection

Agenda
back
more

- Integrates the efforts of four major security and assurance disciplines to support the spectrum of Defense operations

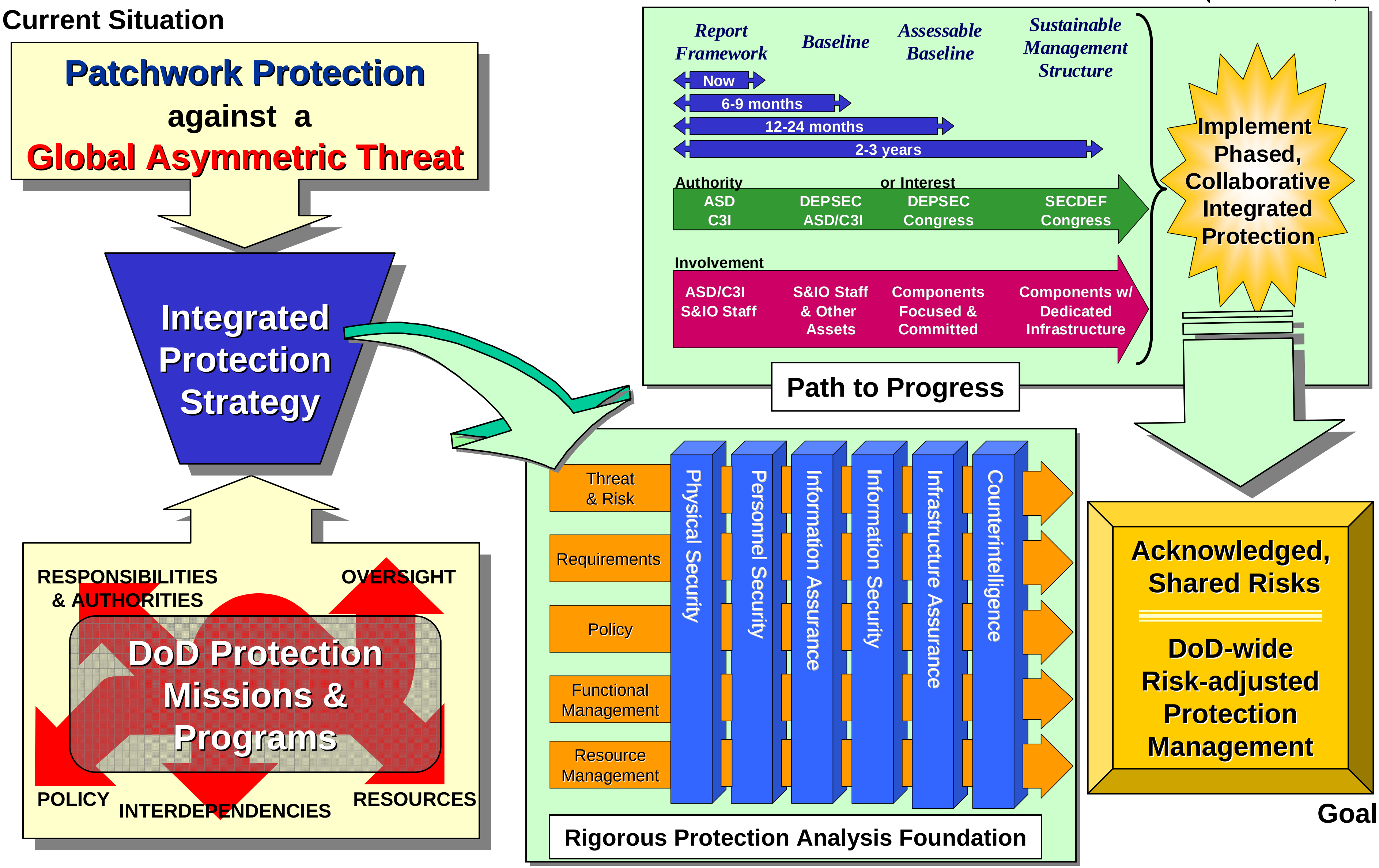
  - Security
    - Policy and oversight of information security, physical security, operational security, personnel security, industrial security, nuclear surety, and SAP/SCI/collateral security
  - Critical Infrastructure Protection (CIP)
    - The identification, assessment, protection, monitoring and operational assurance of cyber & physical mission critical infrastructures essential to the execution of the National Military Strategy.
  - Information Assurance (IA)
    - Protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation
  - Counterintelligence(CI)
    - Protect against foreign intelligence activities and terrorist organizations by conducting CI investigations and examining the illegal transfer of critical defense technologies and intrusions into DoD information systems and terrorism

Integrated Protection

Agenda

back

more



Current Situation

Patchwork Protection
against a
Global Asymmetric Threat

Integrated Protection Strategy

RESPONSIBILITIES & AUTHORITIES

OVERSIGHT

DoD Protection Missions & Programs

POLICY

INTERDEPENDENCIES

RESOURCES

Report Framework | *Baseline* | *Assessable Baseline* | *Sustainable Management Structure*

Now

6-9 months

12-24 months

2-3 years

Authority or Interest

ASD C3I	DEPSEC ASD/C3I	DEPSEC Congress	SECDEF Congress

Involvement

ASD/C3I S&IO Staff	S&IO Staff & Other Assets	Components Focused & Committed	Components w/ Dedicated Infrastructure

Implement Phased, Collaborative Integrated Protection

Path to Progress

Threat & Risk

Requirements

Policy

Functional Management

Resource Management

Physical Security

Personnel Security

Information Assurance

Information Security

Infrastructure Assurance

Counterintelligence

Rigorous Protection Analysis Foundation

Acknowledged, Shared Risks

DoD-wide Risk-adjusted Protection Management

Goal

Integrated Protection Critical Shortfalls

Agenda

back

Critical Infrastructure Protection	- Government/Commercial/Private sector synergy - Personnel for Component CIP efforts	- Focus on Warfighter Requirements & Readiness - Information Sharing - Institutionalization of CIP - Resource Visibility - Physical & Cyber Interdependencies - Delineate CIP, COOP, COG and AT requirements and responsibilities	- Infrastructure Mapping - Infrastructure Visualization - Risk Management and Decision Support Tools
Information Assurance	- Systems Administrators - Awareness and Training - Defense-wide Information Assurance Program staffing	- Risk and Network Mgt. - Legal Framework - Strategic Investment Plan	- Attack Sensing & Warning Tools - Defense-in-Depth - PKI Scalability - Secure COTS
Security	- Security Awareness - Cyber Investigations	- New Security Paradigm ***Integrated Protection*** - Personnel Security	- Integrated Risk Management Standards & Tools
Counterintelligence	- Force Protection - Research & Technology Protection - Information Infrastructure Protection - CI analysts/Agents with Area/Language expertise	- CI Field Activity - Force Protection Response Group - Integrated Protection (Risk-based CI) - National Protection Priorities (Crown Jewels)	- RDT&E Support to CI - Secure Information Sharing of CI SAP Information - National Foreign Visitor System Modernization - DoD CI Information System
Information Operations	- IO Career Path	- IO Integration w/Ops - PSYOPS/EW - Overprotection - Intelligence Support	- CNA Tools - Measures of Effectiveness

Security

Agenda
back

- Programs designed to ensure the security of DoD collateral, Sensitive Compartmented, nuclear, and Special Access Program information, physical assets, national security operations, personnel reliability, and supporting industrial security efforts
- Security activities are conducted under the authorities granted in multiple Executive Orders and National Security Decision Directives.
- ASD C3I provides policies and oversight.
  - DEPSECDEF is the co-chair of the interagency Security Policy Board.
  - DoD is Executive Agent for the National Industrial Security Program.
  - DoD Components plan, program resources, and execute.

Critical Infrastructure Protection (CIP)

Agenda

back

- The identification, assessment, protection and real-time monitoring of *cyber & physical* mission critical infrastructures essential to the execution of the National Military Strategy.

- Conducted under the following authorities -
  - 1996 - EO 13010 - Critical Infrastructure Protection (CIP)
  - May 98 - Presidential Decision Directive 63, Critical Infrastructure Protection (CIP)
  - Nov 98 - DoD CIP Plan, response to PDD-63
  - Jan 00 – National Plan for Critical Information Systems Protection

- ASD(C3I) is the DoD Critical Infrastructure Assurance Officer
  - Responsible for assuring the reliable operation of ***cyber and physical*** infrastructures required to support the full spectrum of Defense operations.

Information Assurance (IA)

Agenda

back

- IA protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

- IA is conducted under the following authorities -.
  - Computer Security Act of 1987
  - National Security Directive 42 (NSD-42), 1990
  - Deputy Secretary of Defense Memorandum, “Management of the Department of Defense (DoD) Information Assurance Program,” January 30, 1998
  - Presidential Decision Directive 63, Critical Infrastructure Protection, May 1998

- ASD C3I provides IA direction and assigns responsibilities for secure, interoperable information capabilities that meet both DoD warfighting and business needs and provides security countermeasures required to secure the GIG architecture.

Counterintelligence (CI)

Agenda

back

- Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations , or international terrorist activities.

- CI Operations conducted under the authority of E.O. 12333
  - Conducted by Army MI, Navy NCIS, AF OSI, USMC CI, and the CI offices of DIA, DSS, DTRA, NSA and NRO

- C3I plans, programs and oversees: services execute
  - Only services can conduct investigations and operations
  - CI has key role in:
    - Force protection
    - Technology protection
    - Critical Infrastructure Protection

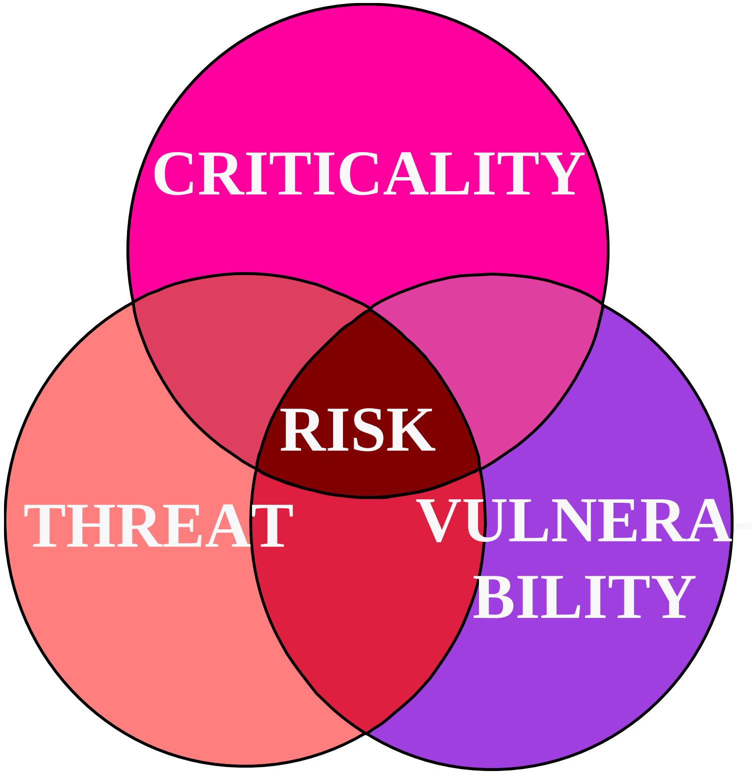
Security: What Has Been Done

Agenda
back
more

- Synergized Collateral and Special Access Program Security Rules
- Developed Plan to Address Periodic Reinvestigation Backlog
- Revised Policies affecting Industrial Security, Nuclear Security, Physical Security, Information Security, Arms Control, Acquisition System Protection
- Revitalized DoD’s Security Education and Training Program
- Developed a Security Plan for the Pentagon

Security: Shortfalls

- Lack of transparency in implementation of security rules.
- Inconsistencies in interpretation of adjudicative standards.
- Personnel Security Investigations are untimely/non-responsive to customer needs.
- Insufficient well-trained security professionals.
- Insufficient security awareness in DoD.



Security: What Needs To Be Done

Agenda

back

- Synergize SCI Security Rules with SAP and Collateral
- Reduce Pending Backlog at DSS
- Consolidate Adjudication Facilities For Uniformity in Decisions
- Develop a Joint Security Training Consortium
- Extend policies to Address Insider Threat (SBU, Trustworthiness)
- Leverage technology to enhance Physical Security Issues Affecting Nuclear Security and Anti-Terrorism efforts
- Establish a strong security framework to deal with the challenges of globalization while facilitating Allied cooperation

CIP: What Has Been Done

- Initiated CINCs Outreach Program based on Y2K lessons-learned
- Developed methodology for analysis of defense infrastructures
- Initiated characterization of defense infrastructures
- Conducted several prototype regional vulnerability assessments, validating viability of concept
- Initiated development of DoD CIP policy and implementing directives
- Inserted CIP considerations into wargaming exercises
- Established link to Federal information & communications CIP efforts
- Initiated quadrilateral and bilateral discussions on common CIP-related issues

CIP : Shortfalls

Agenda
back
more

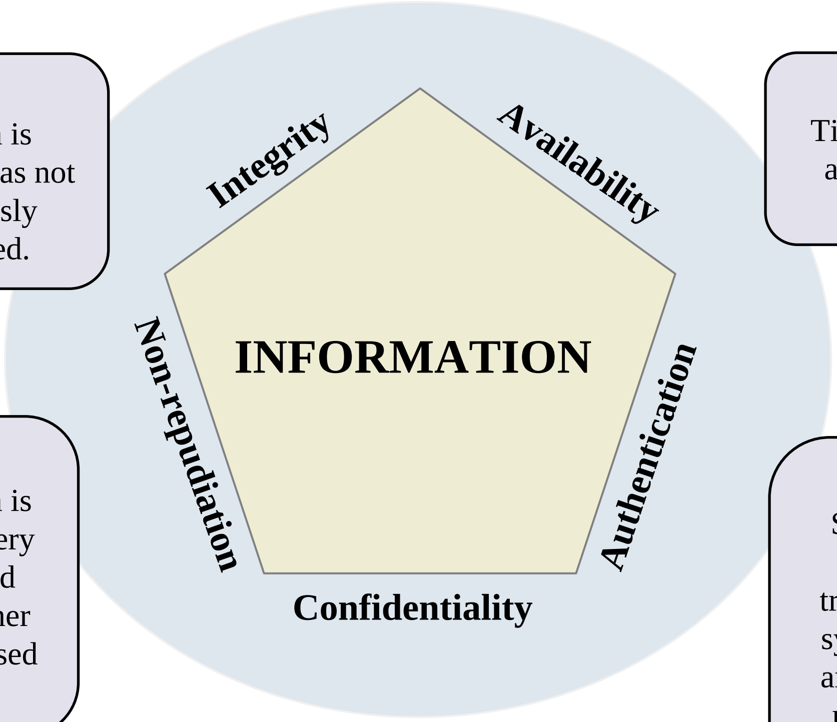
- People
  - Government/Commercial/ Private sector synergy
  - Personnel for Component CIP efforts
- Policy / Process
  - Focus on Warfighter Requirements & Readiness
  - Information Sharing
  - Institutionalization of CIP
  - Resource Visibility
  - Physical & Cyber Interdependencies
  - Delineate CIP, COOP, COG and AT requirements and responsibilities
- Technology / Material
  - Infrastructure Mapping
  - Infrastructure Visualization
  - Risk Management and Decision Support Tools

CIP: What Needs to be Done

- Formalize process for identification of CINC warfighter requirements
- Continue analysis of defense infrastructures, expanding to OCONUS based infrastructures
- Institutionalize CIP in Doctrine, Policy, Requirements and PPBS Process
- Promote integration across all DoD programs including Anti-Terrorism, COOP and COG
- Strengthen cooperation and collaboration in assurance of National Defense Infrastructure (NDI)
- Understand DoD interdependencies on non-defense infrastructures
- Expand and accelerate CIP awareness to include other governments & international /multinational organizations
- Develop technology solutions for supporting CIP requirements

Elements of Information Assurance

Agenda
back
more



INTEGRITY
Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

AVAILABILITY
Timely, reliable access to data and information services for authorized users.

NON-REPUDIATION
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

AUTHENTICATION
Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information.

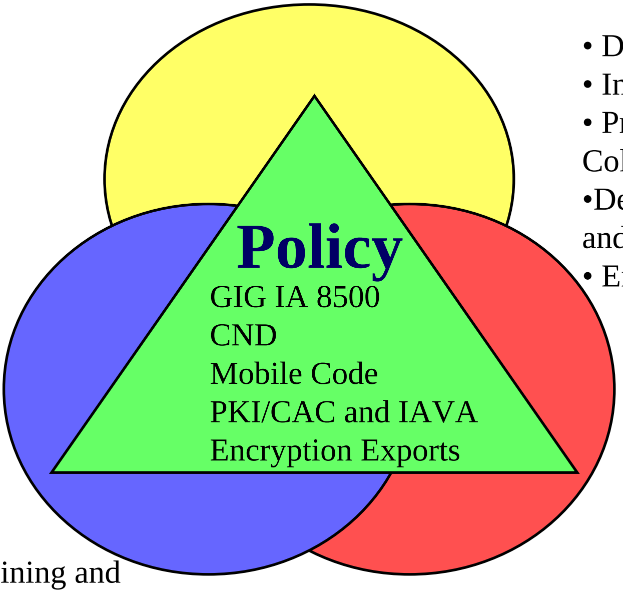
CONFIDENTIALITY
Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Source: NSTISSP

IA: What Has Been Done

Agenda
back
more

Defense-in-Depth Approach



Technology

- Obtained community acceptance of Defense-in-Depth Security Model
- Deployed Intrusion Detection Technologies
- Built Strategic Partnership with Industry
  - Security-enabled Commercial Products
  - Open Security Framework
- Developed Public Key Infrastructure Roadmap
- Increased Availability of IA Products and Services
- Provided R&D for Real-time Monitoring, Data Collection, Analysis, and Visualization
- Developed IA technical framework, common criteria, and NIAP evaluations
- Engaged International Partners

Personnel

- Conducted Human Resources IPT
- Conducted Information Assurance Training and Awareness for All Computer Users
- Certified Personnel Performing Key Functions - e.g., System Administrators
- Developing Career Field Management - Focus on Retention
- Expanded use of Military Reserves
- Established Academic Centers of Excellence / Instructors in Military Academies

Operations

- Created and Implemented the Information Assurance Vulnerability Alert process
- Implemented the INFOCON Process
- Created Service and Agency Computer Emergency Response Teams
- Created the JTF-CND
- Implemented a Real-time Network Monitoring and Reporting Structure
- Integrated Red Teaming
- Institutionalized coordination with NIPC, FEDCIRC, and Intelligence Communities

IA: Critical Shortfalls

- **Funding for highest priority Defense in Depth capabilities to**:
  - develop and employ Global Networking high speed security devices
  - acquire latest secure Wireless technologies
  - replace aging STU-III system with modern Secure Terminal Equipment (STE)
  - deploy Cyber Attack Sensing and Warning nodes and advanced intrusion detection capabilities (FY01 shortfall)
  - fully support the CINCs integration of IA capabilities into warfighting systems, including coalition networks
  - deploy a strong Public Key Infrastructure, including acquisition of PKI enabling applications and directory services
  - develop advanced encryption for new satellite constellation
  - implement IPT recommendations for training, certification, and personnel management for IT/IA (FY01 shortfall)
  - hire and retain IT/Security professionals
  - fully operationalize Joint Task Force for Computer Network Defense
  - sustain International IA Outreach effort
- **Developing and promulgating:**
  - a comprehensive IA Policy Framework supporting the "Global Information Grid" to include a technically comprehensive, system certification and accreditation process and PKI, interoperability/interconnection, and computer network defense policies
  - an integrated IA readiness and compliance process
- **Influencing and empowering industry to develop security products evaluated by National Information Assurance Partnership (NIAP) processes**

IA: What Needs to be Done

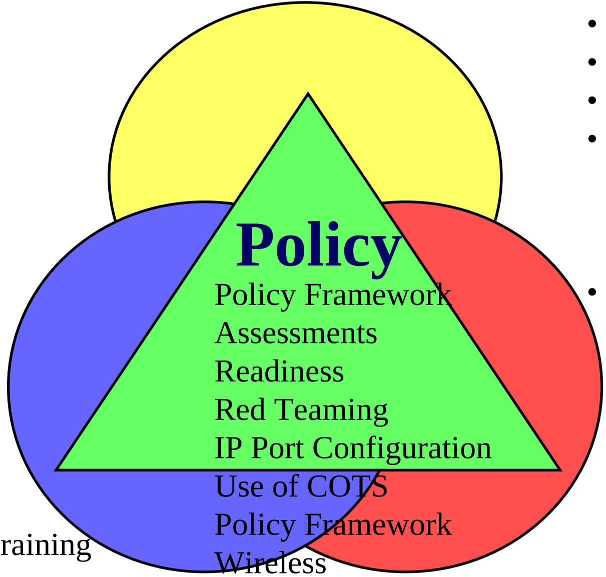
Agenda

back

Defense-in-Depth Approach

Technology

- Fully Document IA Framework in GIG Architecture
- Raise the Security Bar with Industry and Private Sector
- Achieve Public Key Enabling (PKE) of Applications
- More Focused R&D Efforts Across the Community
- Implement Biometrics
- Continue Crypto Modernization
- Achieve Allied Coalition Interoperability
- Fully Integrate Security Management Infrastructure
    - PKE Applications
    - High Assurance PKI
    - Robust Key Management for C3I Systems
- Integrate Wireless Capabilities



Policy

Policy Framework
Assessments
Readiness
Red Teaming
IP Port Configuration
Use of COTS
Policy Framework
Wireless

Personnel

- Conduct Frequent Security Refresher Training
- Provide IA Scholarships
- Implement JVRIO
- Deal with Insider Threat
- Obtain Defense-wide Information Assurance Program Staffing

Operations

- Maintain Continuous Vulnerability Assessment and Control
- Fully Deploy Attack Sensing and Warning Capabilities
- Fully Integrate CND/CNA into Operational Planning
- Increase Red Teaming
- Make IO/IA an Integral Part of Readiness Reporting
- Protect EB/EC Operations

CI: What Has Been Done

Agenda
back
more

- Played key role in developing the “CI-21” National CI Initiative
- Developed Joint CI Analysis Group to enable leveraging of technology for CI analysis
- Created Defense Computer Forensics Laboratory (DCFL) for analysis of media evidence
- Developed new Joint CI Center for expanded CI support to JCS and Combatant Commands
- Fielded the Joint CI Evaluation Office to monitor significant DoD CI investigations and policy
- Created the Defense CI Training Academy to create a new cadre of DoD CI professionals

Agenda
back
more

CI: Shortfalls

- **People**
  - CI analysts/agents with area/language expertise
  - Cyber investigators
- **Policy/Process**
  - Cyber policy for CI
  - National Protection Priorities (CI-21 “Crown Jewels”)
  - CI Field Activity (CIFA)
- **Technology/Materiel**
  - Joint CI Analytical Group (JCAG)
  - DoD CI Information System (DCIIS)
  - National Foreign Visitor System
  - Secure Info Sharing of CI SAP Information

Agenda
back

CI: What Needs to be Done

- Development of DoD CI activities with the "CI-21" National CI structure - policy, programs, personnel
- Creation of a Counterintelligence Field Activity to consolidate Defense CI programs, improve oversight, model DoD with new National CI structure.
- Full IOC of the Joint CI Analysis Group to support DoD CI Technology Protection program and CI investigative and analysis efforts
- Stand up of the Joint CI Center to provide JCS and Combatant Commands with more robust CI support and analysis with reach-back capability for contingencies

Agenda

back

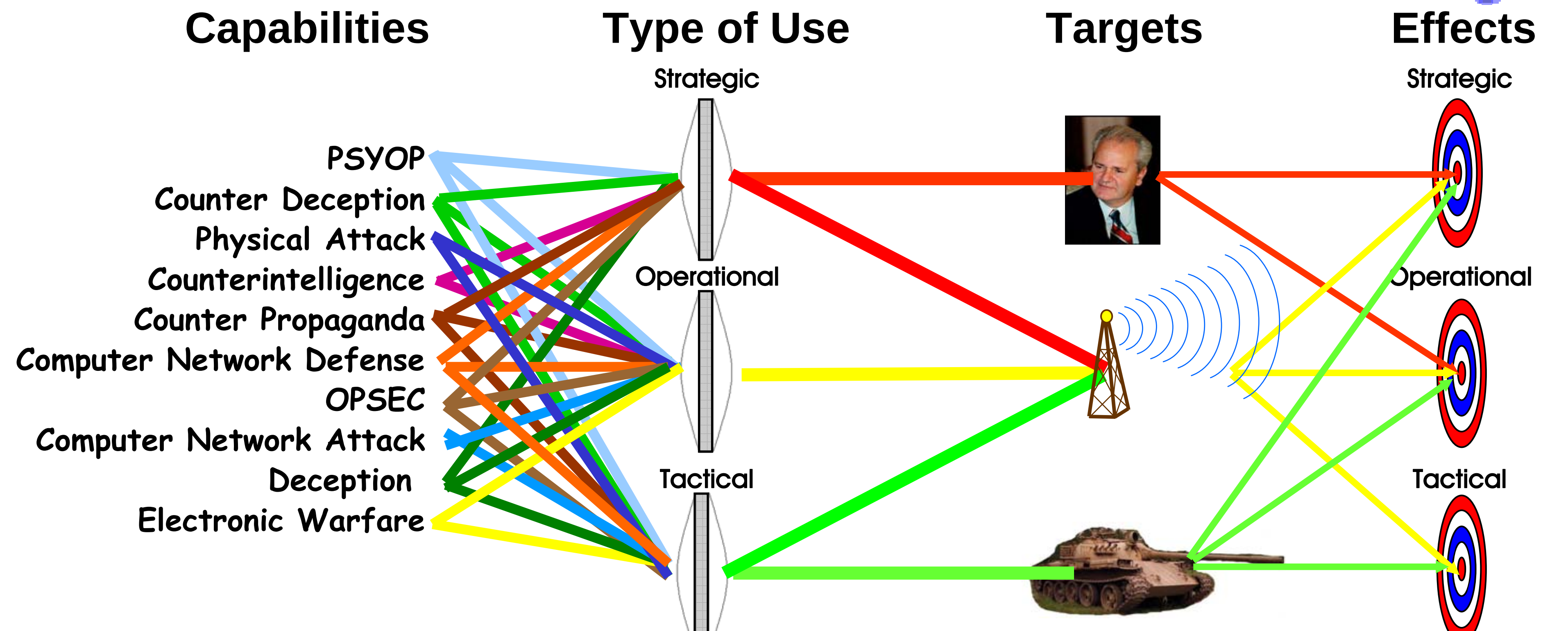
Information Operations

- Actions taken to affect adversary information and information systems while defending one's own information and information systems.

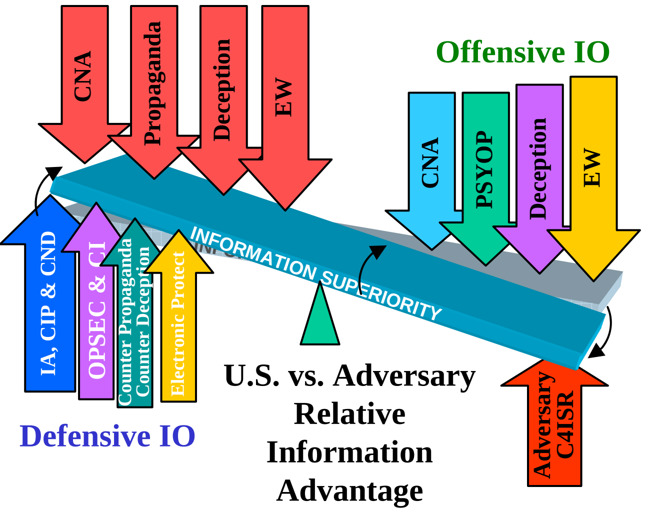
- Conducted under the authorities of the National Security Act of 1947, and Title X

- ASD C3I:
  - Serves as the central POC for DoD and principal staff assistant and advisor to SECDEF and DEPSECDEF for DoD IO
  - Reviews DoD IO plans, programs, and requirements to monitor and evaluate program responsiveness to validated requirements, and to deconflict IO programs
  - Exercises, in coordination with USD(P) and USD(AT&L), oversight of IO matters, to include broad strategy, program and budget review, technology development, security guidance, and education and training
  - Oversees applicable training and career development policy to ensure trained personnel are available to support and execute IO

Information Operations



Intelligence Support



Definition: *Actions taken to affect adversary information and information systems while defending one's own information and information systems*

IO: What Has Been Done

Agenda
back
more

- 1992, (Rev.1996) ASD(C3I) Promulgated DoDD 3600.1:

Information Warfare (IW) Services and Joint Staff establish IW/IO Activities

- 1997 DoD & IC Established Information Operations Technical Center (IOTC)
- 1998 Joint Staff Established Joint Doctrine for IO: Joint Pub 3-13
- 1998 DoD and IC establish the Bilateral IO Steering Group and Work Group
- 1997-2000 Exercises: Eligible Receiver, Evident Surprise, Steel Puma
- 1998-2000 Real world events: Solar Sunrise, Moonlight Maze, Nobel Anvil (Kosovo), Love Bug
- 1998 stood up JTF Computer Network Defense (JTF CND)
- 1999 ASD(C3I) establishes the Defense IO Council
- 1999 USSPACECOM assumes CND Mission and JTF CND
- 1999 Army and Air Force stand up operational IO Battalions/Wings
- 2000 Naval Security Command Group becomes the Navy’s Executive Agent for IO
- 2000 ASD(C3I) IO Broad Area Review - Established R&D Resource Baseline
- 2000 ASD(C3I) IO Critical Program Information Audit
- 2000 DSB Study on PSYOP - Identifies critical deficiencies in PSYOP
- 2000 USSPACECOM Assumes Computer Network Attack (CNA) mission

IO: Shortfalls

PEOPLE:

- **Blending Old Skills with New Skills**
  - Training, retention, and career path development is weak

POLICY/PROCESS:

- **National Policy -** Need to enhance PDDs 56, 63, 68 into overarching IO Strategy
- **Intelligence Support to IO -** Greater intelligence necessary for capability development, computer network order of battle, PSYOP planning and BDA
- **Integration With Operations -** Commanders and planners not familiar with capabilities and doctrine which often results in IO options being overlooked in the strategy-to-task process
- **Over Protection -** Unnecessarily high and inconsistent protection measures hinder R&D to warfighter implementation

TECHNOLOGY/MATERIEL:

- **PSYOPS Neglected -** Insufficient resources to modernize, requirements are outdated, lacks sufficient Intel support
- **Electronic Warfare (EW) Atrophy -** No Joint EW technology road map, follow-on concept for EA-6B not defined
- **Measures of Effectiveness -** few measures of effectiveness exist to reliably predict effects and to conduct battle damage assessment.

IO: What Needs to be Done

Agenda

back

PEOPLE:

- Oversee DoD component plans for IO related career path development and training

- **POLICY/PROCESS:**
- Support USD(P) efforts with NSC and interagency to refine national policy and guidance with respect to IO
- Work to improve and expand intelligence support for Information Operations on par with national efforts like counter-terrorism and counter-proliferation of WMD. This is especially critical for PSYOP, and EW related activities
- Support exercises, experiments, modeling and simulation of IO capabilities to improve doctrine, integration, and planning
- Develop clear guidance on the protection required for sensitive IO programs
- Develop a plan to re-look how PSYOP and Public Information can be used more effectively to achieve the combat commander’s objectives

TECHNOLOGY/MATERIEL:

- Emphasize the need for state-of-the-art Electronic Warfare capabilities to support Information Operations. Push for the development of new concepts for accomplishing the Department’s Electronic Warfare mission and a technology roadmap
- Develop a standard method to determine Measures of Effectiveness to provide CINC’s the ability to predict accuracy and probability of kill for non-kinetic weapons

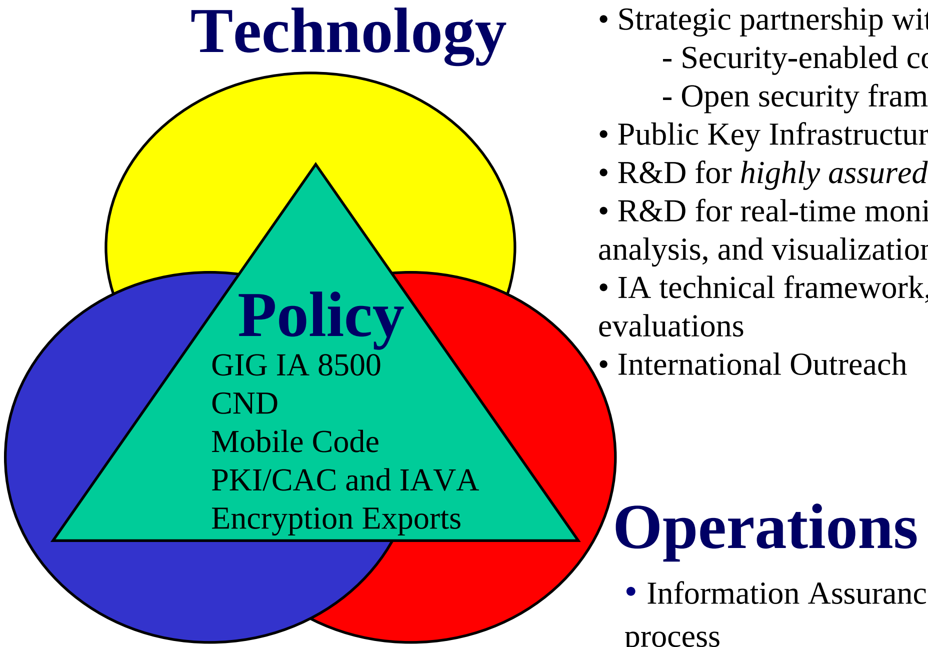
Keeping the Momentum Going:

Defense-in-Depth Initiatives

Agenda

back

- Community adoption of Defense in Depth security model
- Deployment of intrusion detection technology
- Strategic partnership with industry
  - Security-enabled commercial products
  - Open security framework
- Public Key Infrastructure roadmap
- R&D for *highly assured* products and systems
- R&D for real-time monitoring, data collection, analysis, and visualization
- IA technical framework, common criteria, and NIAP evaluations
- International Outreach



- Human Resources IPT
- Information assurance training and awareness for all computer users
- Certification of personnel performing key functions - e.g., System Administrators
- Career field management - focus on retention
- Expanded use of Military Reserves
- Academic Centers of Excellence / Instructors in Military Academies

- Information Assurance Vulnerability Alert process
- INFOCON process
- Service and Agency Computer Emergency Response Teams
- Creation of JTF-CND
- Real-time network monitoring and reporting structure
- Red Teaming
- Coordination with NIPC, FEDCIRC, and Intelligence Communities

Keeping the Momentum Going:

CI-21

Agenda

back

- World Changed, new Threats emerged, U.S. CI agencies caught in Cold War organization, fragmented, compartmented, inflexible
- CI 21 created to establish a National CI system to deal with globalization, the cyber age, and asymmetric threats on a proactive basis
- Establishes “CI Board of Directors” - Dir. FBI (Chair), Dep. Dir. CIA, DepSecDef, Dep. Attorney General. (In coordination with NSC Deputies Committee)
- Creates a National CI Executive - 100% focused on CI Issues
- Makes DoD a co-equal with FBI & CIA in new National CI System

Keeping the Momentum Going:

Responsive Personnel Security

Agenda

back

- Revitalize training and education programs address needs of personnel security community.
- Identify career-wide requirements to ensure continuous professional development.
- Monitor the “spend plan” vice cases as a means of addressing PSI backlog.
- Update DoD 5200.2-R to insure execution of a uniform policy.
- Establish virtual linkage between the CAFs and JPAS.
- Create better standards for special access programs.
- Triage PSI backlog i.e. prioritize cases to insure most critical are processed first.
- Monitor implementation of the Smith Amendment.

Tackle some Stubborn Problems:

Critical Infrastructure Protection

Agenda

back

- Formalize process for identification of CINC warfighter requirements
- Continue analysis of defense infrastructures, expanding to OCONUS based infrastructures
- Institutionalize CIP in Doctrine, Policy, Requirements and PPBS Process
- Promote integration across all DoD programs including Anti-Terrorism, COOP and COG
- Strengthen cooperation and collaboration in assurance of National Defense Infrastructure (NDI)
- Understand DoD interdependencies on non-defense infrastructures
- Expand and accelerate CIP awareness to include other governments & international /multinational organizations
- Develop technology solutions for supporting CIP requirements

Tackle some Stubborn Problems:

Integrated Protection

Agenda

back

- Annual DoD Protection Budget Exceeds $8 Billion
- Department has Little Understanding of:
  - Impact of new/emerging threats for the protection disciplines (e.g., physical security; cyber security;personnel security; classified information security; counterintelligence)
  - Interrelationship of physical, personnel and cyber vulnerabilities
  - How DoD Components determine acceptable risk
  - Effectiveness of protection policy, practices, expenditures vis-à-vis threats
- There is Growing Need to Understand and Employ Protection Disciplines in an Integrated Way
- Integrated Protection Objective
  - Develop collaborative management process
  - Assess the effectiveness of DoD interrelated protection disciplines, missions and programs
  - Gain better visibility into protection resources
  - Evaluate the impact of risk trade-offs and budget trade-offs across multiple DoD protection disciplines

Tackle some stubborn problems:

Countering the Insider Threat

Agenda

back

- Insider threat to DoD information systems is real

Sources of Information Systems Security/Usage Problems	Nature of the Threat	Probable Damage	Frequency
Maliciousness (disgruntled employee or agent provocateur)	• Capability to Inflict Damage or Destroy, Compromise Intelligence • Enhances Potential for Outside Attacks • Deliberate Intent	Substantial	Unknown
Disdain of Security Practices	• Capability to Inflict Damage • Enhances Potential for Outside Attacks • Unintentional	Unknown	Unknown
Carelessness			
Ignorance			

- Threat is to closed systems processing classified and open systems processing unclassified information; each is based on the use of the same vulnerable COTS products
- High impact actions
  - Security education, training and awareness
    - Emphasize and reinforce practicing security basics, first
    - Establish minimum education and training requirements for security
  - Personnel management
    - Reinforce workplace behavior expectations
    - Develop a Personnel Security Strategic Plan
  - Information technology
    - Use effectively the technology already at the Department’s disposal
    - Seek R&D solutions with greatest immediate operational relevancy

Tackle some stubborn problems:

Technical Security Challenges

Agenda

back

- Acknowledge threat as real vice theoretical.
  - example: recovered eavesdropping devices at DoS
- Technology migration from analog to digital brings new range of challenges.
- Challenges increased by break-up of phone monopoly leading to smaller segments and more devices.
- Technology shifting from large scale to micro-scale technologies - ex: smart dust particles.
- Technology for retention of data shifting - ex: holographic storage.
- Production methodology changing from “hardwired” and chip production to lab-grown devices.

Tackle some stubborn problems:

Intelligence Support to IO

Agenda

back

Amend Presidential Decision Directive 35 to include intelligence support to IO

- IO depends on significant intelligence support to be successful. Broad range of needs include:
  - Highly detailed data on technical parameters of global information networks
  - In-depth knowledge of human factors influencing decision making processes

- Increased Investment and Priority for Analysis & Collection needed to plan and execute both offensive and defensive IO
  - Develop cadres of analytical expertise specializing in support to technical and human factors aspects of IO
  - Develop new intel sources and methods to collect against IO requirements.
  - Develop Standard process for IO target analysis & MOE/BDA

Information Assurance Challenges

- Interconnected, interdependent systems - “Shared Risk” underscores need for broad understanding of threats and vulnerabilities
- Move beyond Information Security (Protection of information) to Information Assurance (Full spectrum protection)
- Security-enabled commercial products as a basis for solution(s)
- Global *Interoperable* Security Management Infrastructure
- Cyber situation awareness to assure confidence in the underlying network
- Ensure tight integration with other assets of the GIG

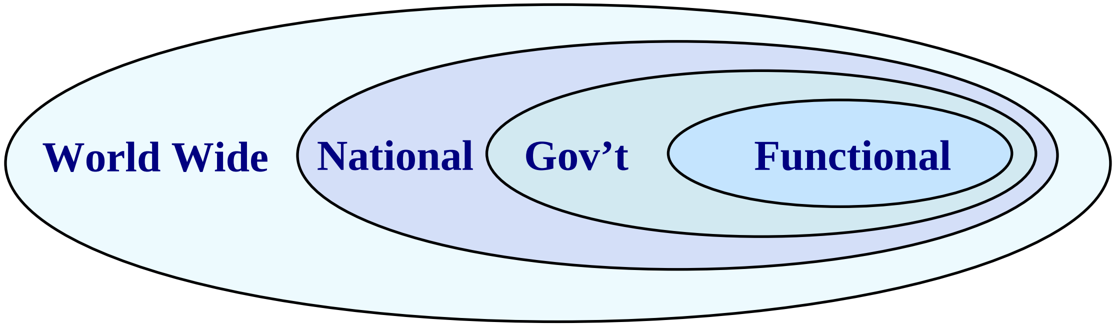
Interlocking Communities

Agenda

back

Served by Interlocking (and Interdependent) Information Infrastructures:

Electronic Commerce
Electronic Mail
Electronic Data Interchange
Electronic Funds Transfer
File Transfer
Information Search/Retrieval



Requiring:

Basic Information Assurance Services

System Availability **User Identification & Authentication**

Data Integrity **Data Confidentiality** **Transaction Non-Repudiation**

Digital Signature ***Encryption*** ***Key Exchange***

Security Management Infrastructure

What is Electronic Business? (e-business)

The application of industry and government best practices and modern information technology to improve the management and operational processes of the Department

eBusiness has a very broad scope encompassing all DoD business functional areas and most combat support functions:

- Brings together eBusiness stakeholders with needs and capabilities
- Requires application of new business rules and innovative to deliver dramatically improved mission performance, reduced costs and cycle times, and improved quality
- Applies commercial off-the-shelf applications

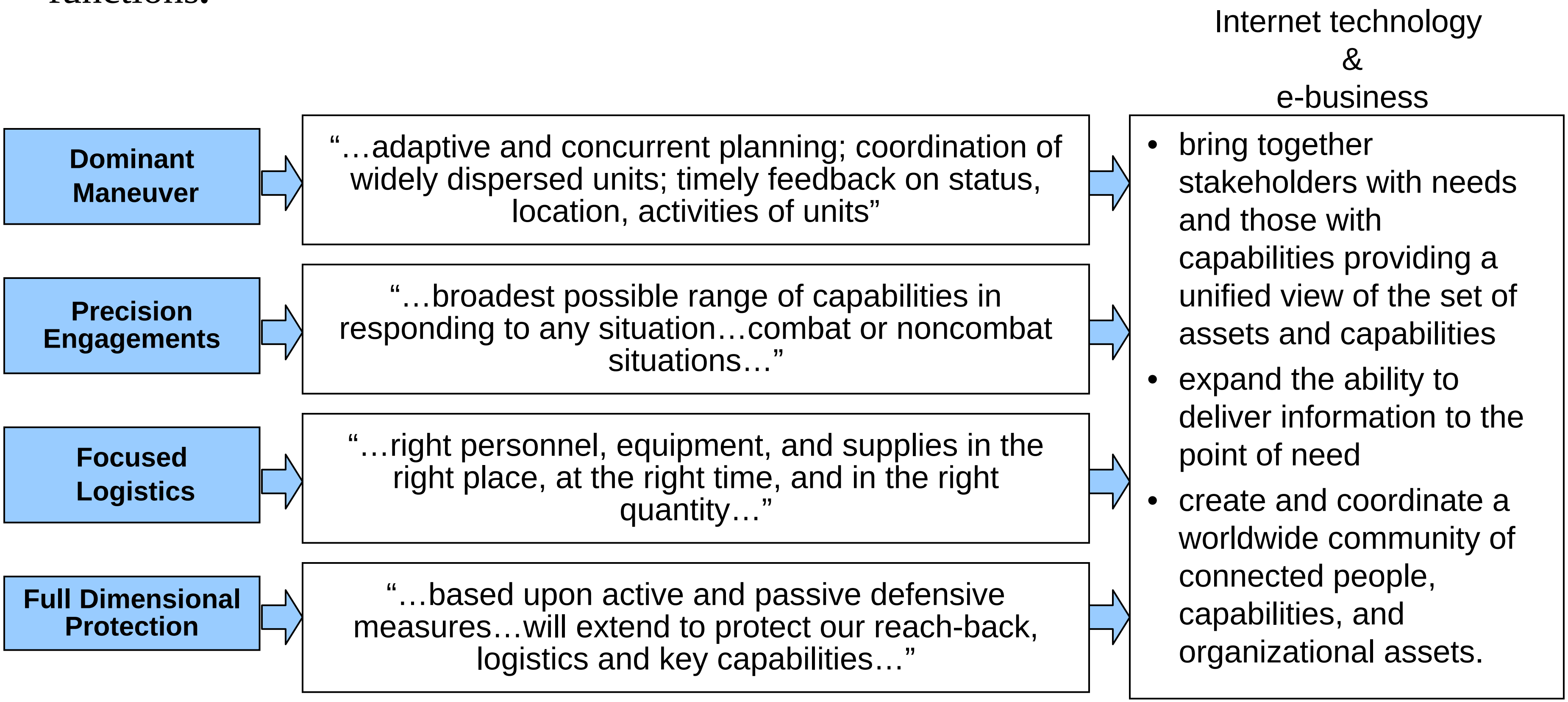
e-Business & Joint Vision 2020

Agenda

back

more

- Beyond often cited cost savings, easy functionality, and customer satisfaction - Joint Vision 2020 requires a network of connected DoD functions.



Internet technology
&
e-business

Dominant Maneuver → "…adaptive and concurrent planning; coordination of widely dispersed units; timely feedback on status, location, activities of units" →

Precision Engagements → "…broadest possible range of capabilities in responding to any situation…combat or noncombat situations…" →

Focused Logistics → "…right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity…" →

Full Dimensional Protection → "…based upon active and passive defensive measures…will extend to protect our reach-back, logistics and key capabilities…" →

- bring together stakeholders with needs and those with capabilities providing a unified view of the set of assets and capabilities
- expand the ability to deliver information to the point of need
- create and coordinate a worldwide community of connected people, capabilities, and organizational assets.

The Revolution in Military Affairs cannot be accomplished without a Revolution in Business Affairs

What Have We Done to Advance e-Business?

Agenda

back

more

- •Established the CIO as the Principal Staff Assistant for eBusiness
- •Released the Electronic Business/Electronic Commerce (EB?EC) Strategic Plan setting forth the initial eBusness vision, principles, goals, and objectives
- •Issued DoD Directive that established the DoD eBusiness Program prescribing essential policy, roles, and responsibilities
- •Chartered an EB Board of Directors comprised of senior officials tasked to coordinate Department-wide eBusiness implementation and execution
- •Worked with the Congress to implement key eBusiness legislation to provide the foundation for advancing eBusiness across the Department. This legislation includes:
    - •Clinger Cohen Act
    - •Government Performance and Results Act
    - •Government Paperwork Elimination Act

ne Principal Staff Assistant for eBusiness
ategic Plan, that set forth the initial eBusiness vision, principles, goals, and objectives
ess program, prescribing essential policy, roles, and responsibilities
tasked to coordinate Department-wide eBusiness implementation and execution
the foundation for advancing eBusiness across the Department. This legislation includes:

Key e-Business Initiatives

- Created new management framework to improve adoption of eBusiness within the Department
- Established smart card based identification and access card program for DoD
- Developed Wide Area Work Flow / Receipts and Acceptance (WAWF-RA) web-based system that allows DoD contractors and authorized DoD personnel to generate, capture and process invoices and acceptance documents electronically
- Refocusing the Joint Electronic Commerce Project Office (JECPO) to improve the JECPO project life cycle process from project selection to hand-off to a sponsor for deployment.
- Leveraging Commercial Processes
  - Adopting commercial business rules and products
  - Outsourcing
  - Enterprise Resource Planning (ERP)

The DoD e-Management Framework

framework elements collectively support successful e-business implementation

Agenda

back

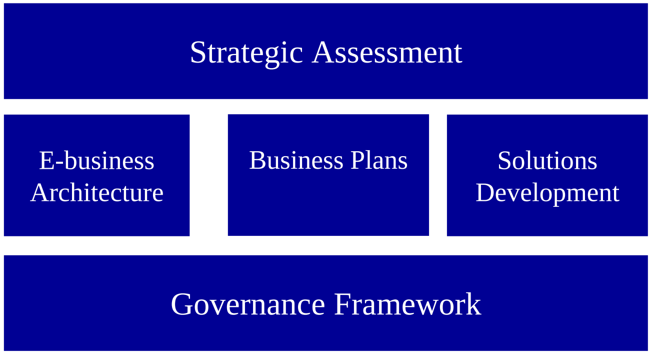
more

Strategy

- Strategy creation process
- Methodology followed to create e-business strategy
- Plan for communication and an enforcement strategy

e-Business Architecture

- Scalability
- Vendor neutral
- Security
- Access



Solutions Development

- Business driven cross-organizational requirements
- Documented and repeatable methodology
- Evaluation and testing

Business Plans

- Business line input
- BPR
- Program Management Plan
- Risk Management Plan
- Acquisition Plan

e-Governance

•Mission

•Organization

•Roles and responsibilities

•Processes

•Policies

•Measures

•Content

DoD Smart Card Roadmap

Agenda
back
more

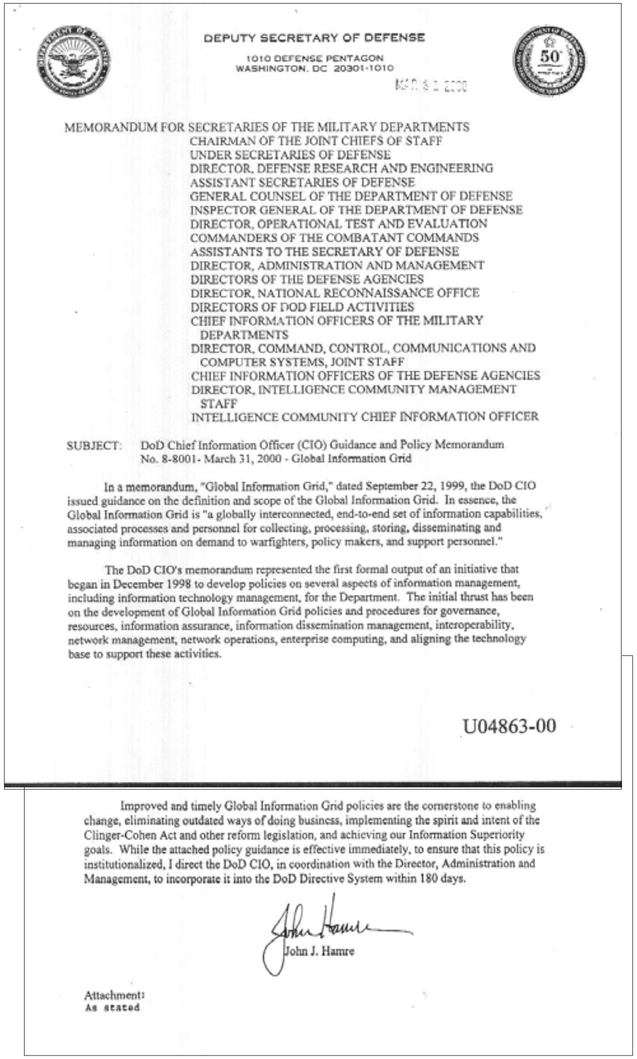
- The card platform will include all relevant media
- This will be the predominant platform for the PKI hardware token
- This “DoD Common Access Card (CAC)” will be the Military and Civilian Identification Card
- We will use DEERS/RAPIDS platform for card maintenance
- DoD (OSD/C3I/CIO) will head up a configuration control board (with Service Reps) to specify technical allocation of chip
- Space will be allocated on the chip for Services/Agencies specific application
- OSD functional leaders (P&R, Comptroller, C3I, etc.) will convene community panels to develop consensus for data element standardization on chip space

What must be done to further institutionalize e-Business?

- Establish clear strategic vision and focus reengineer on major mission processes
- Implement progressive e-business management framework championed by DepSecDef and top DoD leadership
- Obtain Trusted Commerce through application of Information Assurance
- Provide within the Global Information Grid (GIG) operational architectures that reflect the functional and interfacing process points
- Obtain necessary resource streams to permit effective execution

The Global Information Grid (GIG)

Agenda
back
more



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 3 1 2000

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001- March 31, 2000 - Global Information Grid

In a memorandum, "Global Information Grid," dated September 22, 1999, the DoD CIO issued guidance on the definition and scope of the Global Information Grid. In essence, the Global Information Grid is "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel."

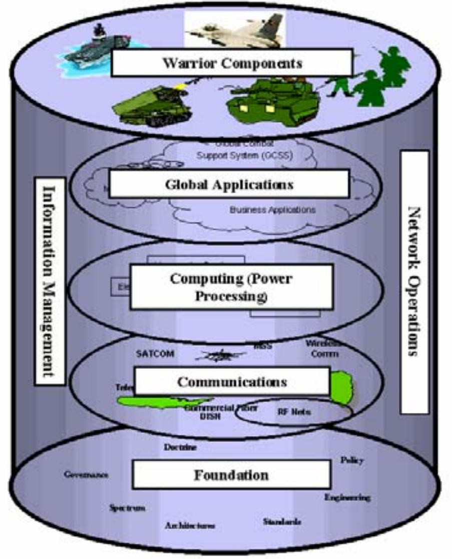
The DoD CIO's memorandum represented the first formal output of an initiative that began in December 1998 to develop policies on several aspects of information management, including information technology management, for the Department. The initial thrust has been on the development of Global Information Grid policies and procedures for governance, resources, information assurance, information dissemination management, interoperability, network management, network operations, enterprise computing, and aligning the technology base to support these activities.

U04863-00

Improved and timely Global Information Grid policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals. While the attached policy guidance is effective immediately, to ensure that this policy is institutionalized, I direct the DoD CIO, in coordination with the Director, Administration and Management, to incorporate it into the DoD Directive System within 180 days.

John J. Hamre

Attachment:
As stated



Global Information Grid

The *globally interconnected*, *end-to-end* set of information capabilities, associated processes and personnel for *collecting, processing, storing, disseminating and managing information on demand* to warfighters, policy makers, and support personnel. The GIG includes all *owned and leased communications and computing systems and services, software (including applications), data, security services* and other associated services necessary to achieve Information Superiority. It also includes *National Security Systems* as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all *Department of Defense, National Security, and related Intelligence Community* missions and functions (strategic, operational, tactical and business), in *war and in peace*. The GIG provides capabilities from all operating locations (*bases, posts, camps, stations, facilities, mobile platforms and deployed sites*). The GIG provides ***interfaces to coalition, allied, and non-DoD users and systems***.

The GIG is a major DoD Transformation initiative

Global Information Grid

Agenda
back
more

Globally interconnected, information capabilities, associated processes and personnel for

collecting *processing*
storing *disseminating*
managing information

on demand to warfighters, policy makers, and supporters

The GIG includes -

all owned and leased communications
computing systems and services
software, applications and data
security services

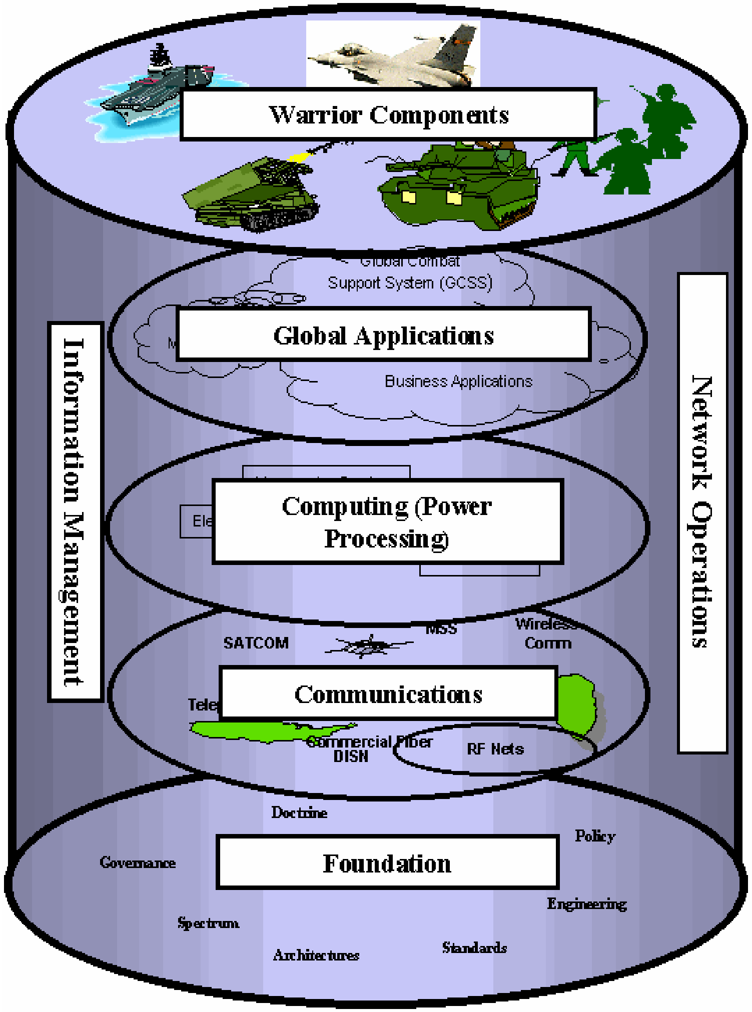
The GIG supports –

Department of Defense
National Security activities
Intelligence Community
missions in war and in peace.

The GIG provides capabilities from all operating locations -

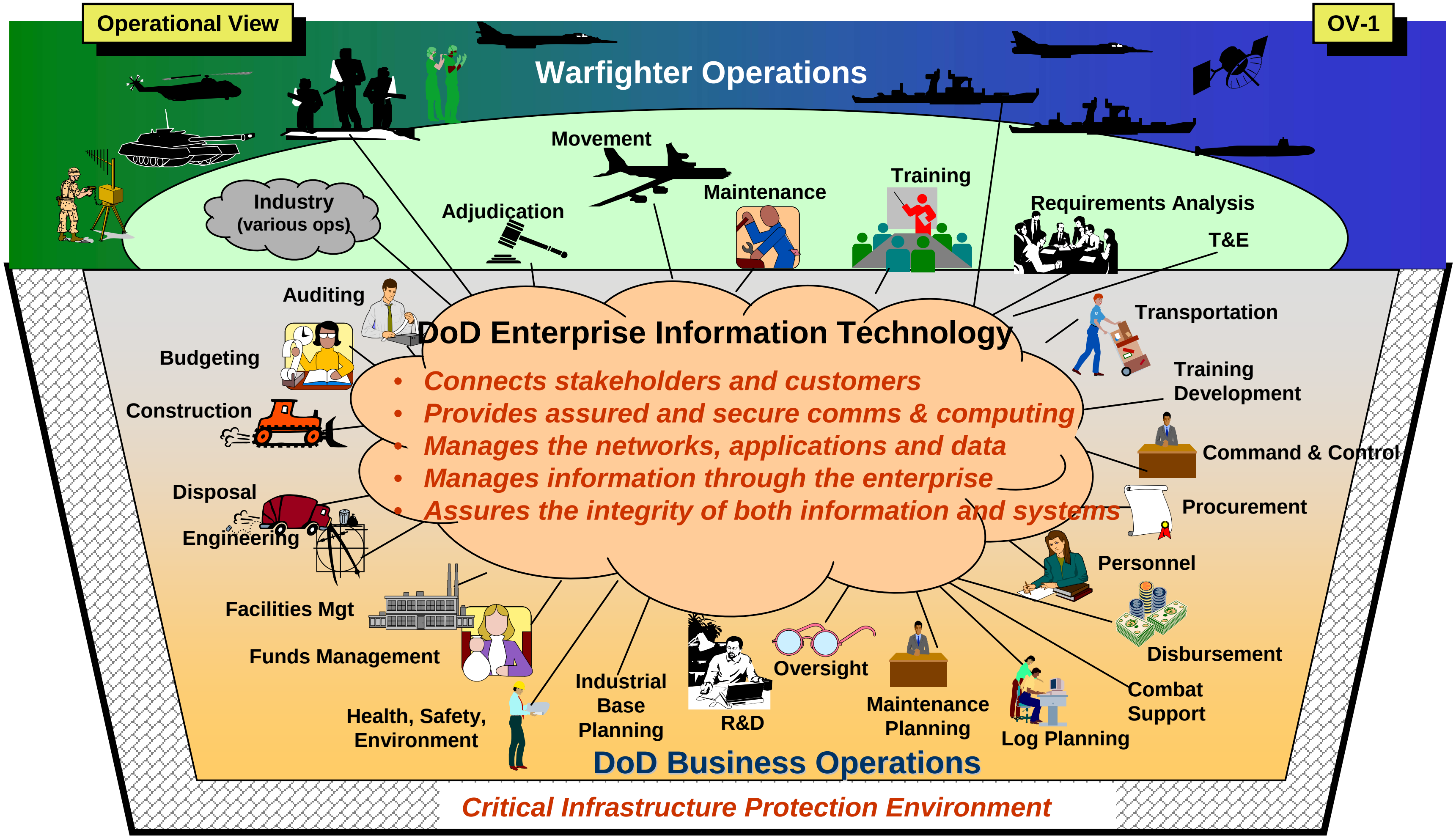
bases *posts* *camps* *stations*
facilities *mobile platforms* *deployed sites*

The GIG provides interfaces to coalition, allied, and non-DoD users and systems



Two Revolutions - One Architecture One GIG

Revolutions In Military and Business Affairs

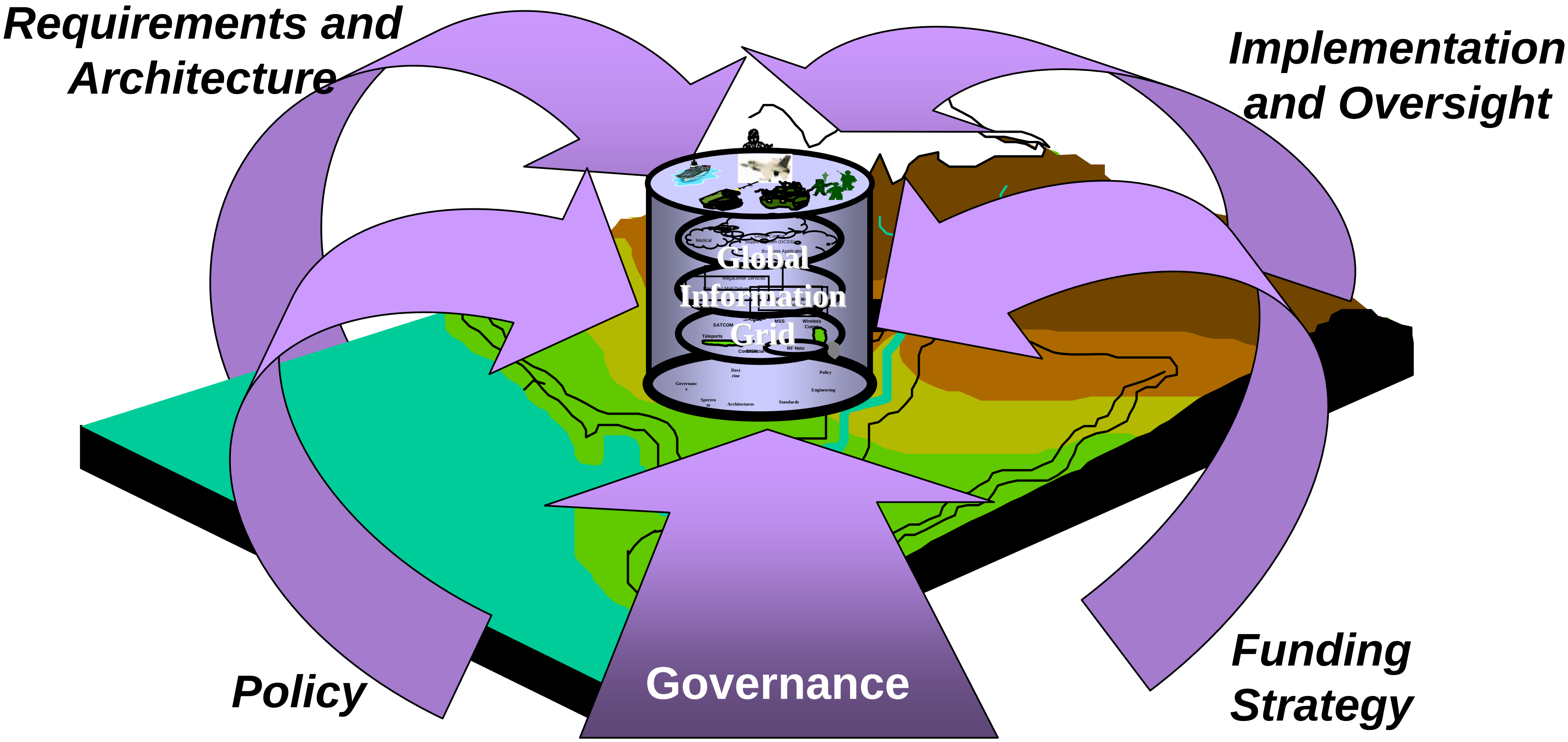


The GIG Campaign Plan

Agenda

back

more



Requirements and Architecture

Implementation and Oversight

Policy

Governance

Funding Strategy

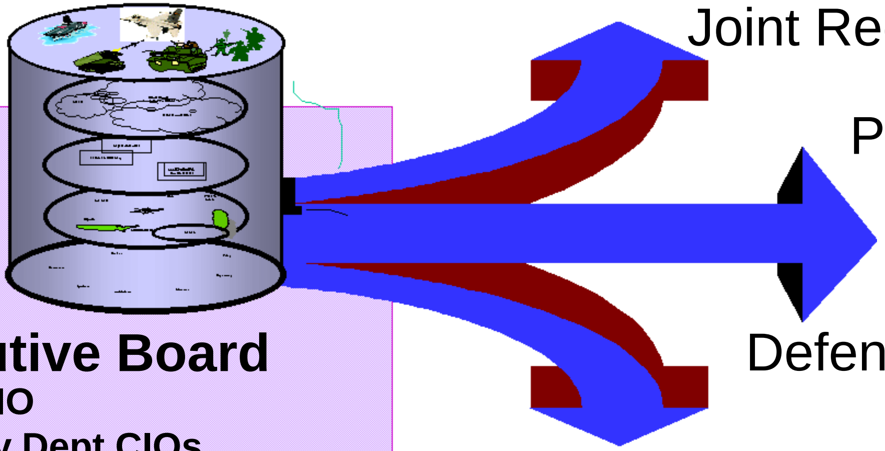
"Develop, maintain, and facilitate the implementation of ***a sound and integrated information technology architecture*** *for the executive agency "*

(Clinger-Cohen Act of 1996, 40 U.S.C. 1425)

How will the GIG Architecture Be Implemented?

Agenda
back
more

Global Information Grid Architecture



Synchronizing DoD Processes

Joint Requirements System

Planning, Programming and Budgeting System

Defense Acquisition System

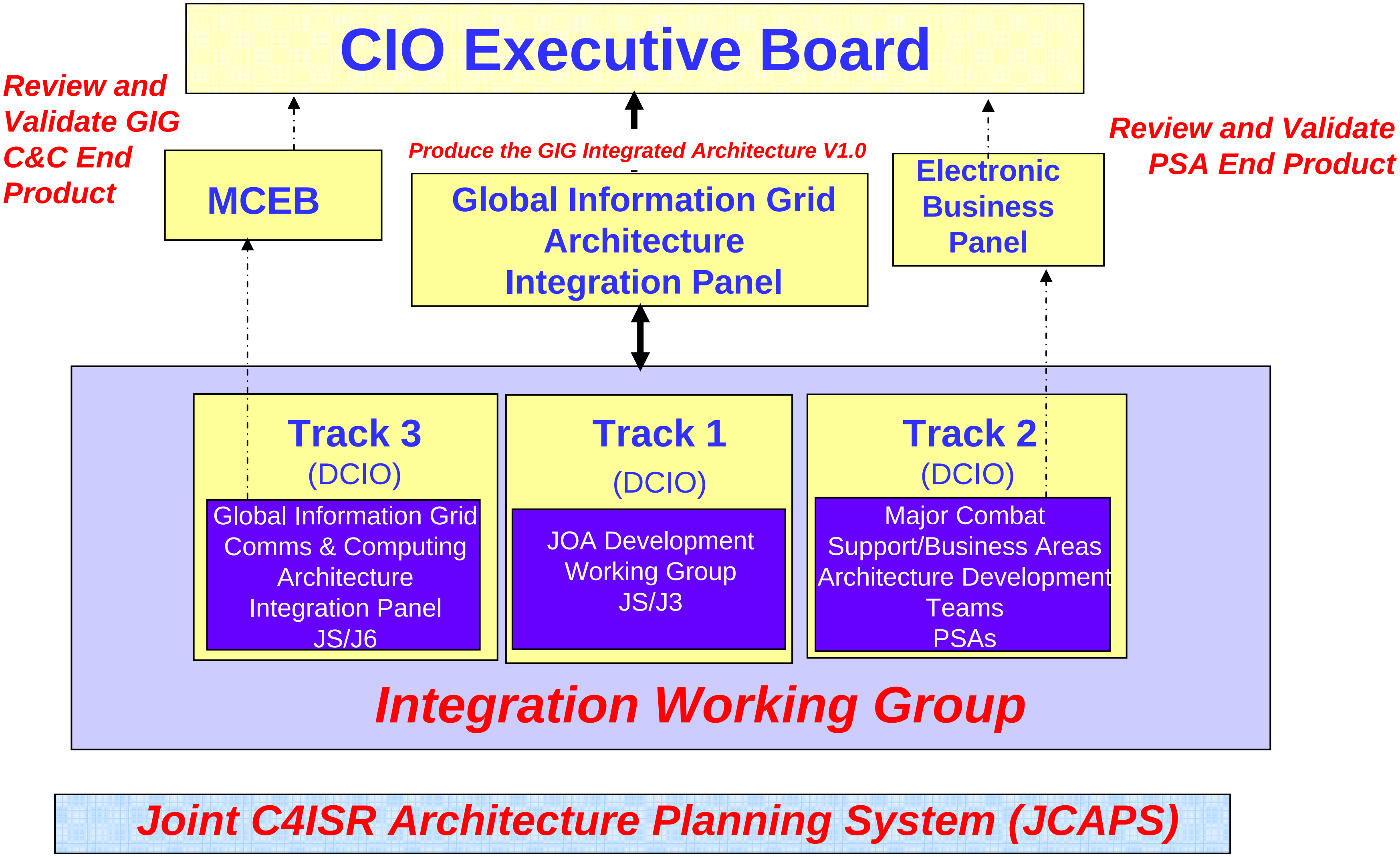
National Foreign Intelligence Program

CIO Executive Board

DoD CIO
Military Dept CIOs
Intell Community CIO
Joint Community CIO
Principal Staff Assts
Joint Forces Cmd CIO
DISA - Technology advisor
NSA - Security advisor

> ***"The Global Information Grid shall be implemented by the acquisition of assets and the procurement of services based on the Global Information Grid architecture"***
>
> ***GIG Overarching Policy, para 4.17***

GIG Architecture Task Organization



CIO Executive Board

Review and Validate GIG C&C End Product

MCEB

Produce the GIG Integrated Architecture V1.0

Global Information Grid Architecture Integration Panel

Electronic Business Panel

Review and Validate PSA End Product

Track 3
(DCIO)
Global Information Grid Comms & Computing Architecture Integration Panel
JS/J6

Track 1
(DCIO)
JOA Development Working Group
JS/J3

Track 2
(DCIO)
Major Combat Support/Business Areas Architecture Development Teams
PSAs

Integration Working Group

Joint C4ISR Architecture Planning System (JCAPS)

One Integrated Architecture: Three Views

Agenda

back

more

Joint Operational Architecture (JOA)

CINC Architectures

Functional Architecture Data

Computing and Comms Templates

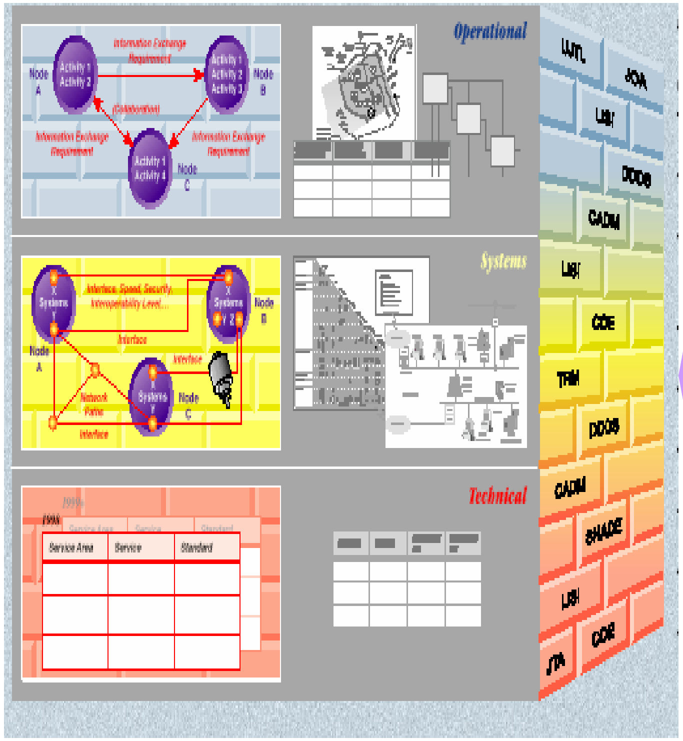
Joint Technical Architecture

C4ISR Architecture Framework - compliant

The Operational View describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission operations.

The Systems View describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational requirements.

The Technical View describes the profile of rules, standards, and conventions governing systems implementation.



Service Enterprise Level Architectures

National Level Architectures

Mandated and Evolving Standards

Model: Joint Task Force

GIG Architecture Version 1.0 Participating Organizations

Agenda
back
more

- DoD CIO/ A&I
- Joint Staff: J3, J6, J4, J2
- OASD(C3I)/C3ISR
- US Army/ DISC4
- Joint Strike Fighter C4IPT
- Joint Theatre Air and Missile Defense Organization (JTAMDO)
- Joint Battle Center (JBC)
- Intelligence Community (IC CIO/ICON)
- DoD Principal Staff Assistants: OUSD(AT&L), OASD(HA), OUSD(C)/DFAS, OUSD(P&R)

GIG Architecture Version 1.0 Product Summary

Agenda

back

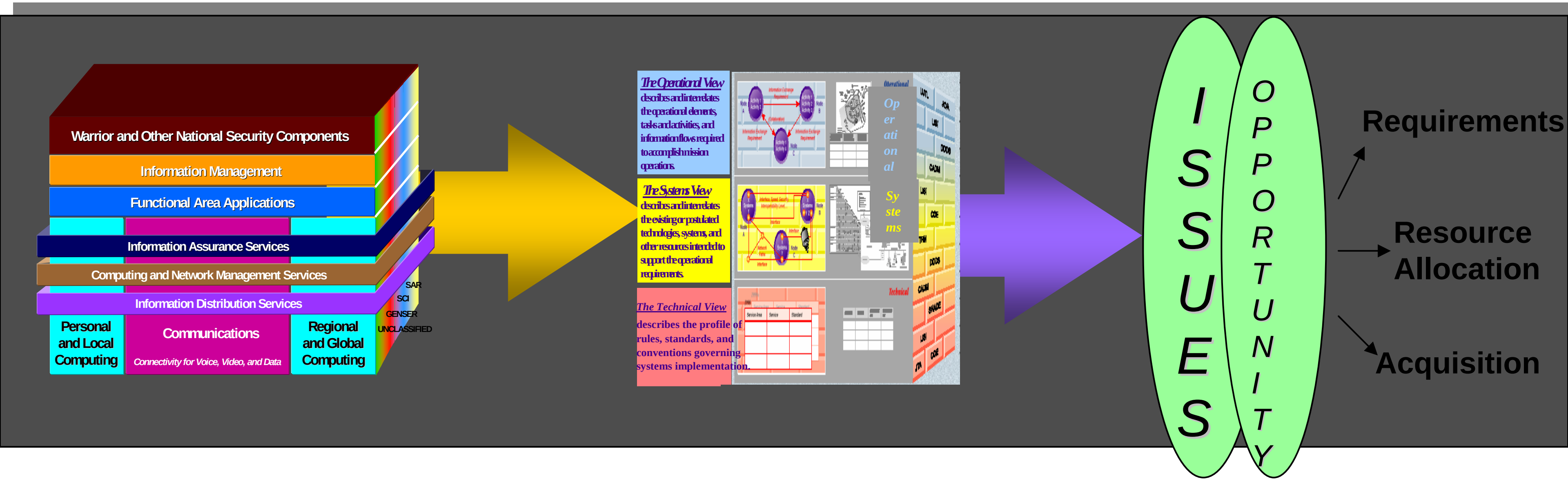
more

- Integrated GIG Architecture Views
  - GIG Operational View
  - GIG Systems View
  - GIG Technical View (Recommended Modifications to JTA and technology forecast)
- Integrated Architecture Dictionary and Style Guide
- Architecture Derived Shortfalls and/or Recommendations to Influence Investment Strategy
  - Focus on selected issues
- Lessons Learned
- GIG Architecture Version 2.0 Plan
- Distribution - Provide on CD ROM(s) Jan 2001

GIG Decision Opportunity Process

Agenda
back
more

A decision process to prioritize and decide the issues that surface as a result of the GIG architecture effort.



Warrior and Other National Security Components
Information Management
Functional Area Applications
Information Assurance Services
Computing and Network Management Services
Information Distribution Services
Personal and Local Computing
Communications
Connectivity for Voice, Video, and Data
Regional and Global Computing
SAR
SCI
GENSER
UNCLASSIFIED
Operational
Technical
Operational
Systems
ISSUES
OPPORTUNITY
Requirements
Resource Allocation
Acquisition

The Operational View describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission operations.

The Systems View describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational requirements.

The Technical View describes the profile of rules, standards, and conventions governing systems implementation.

IT Issues

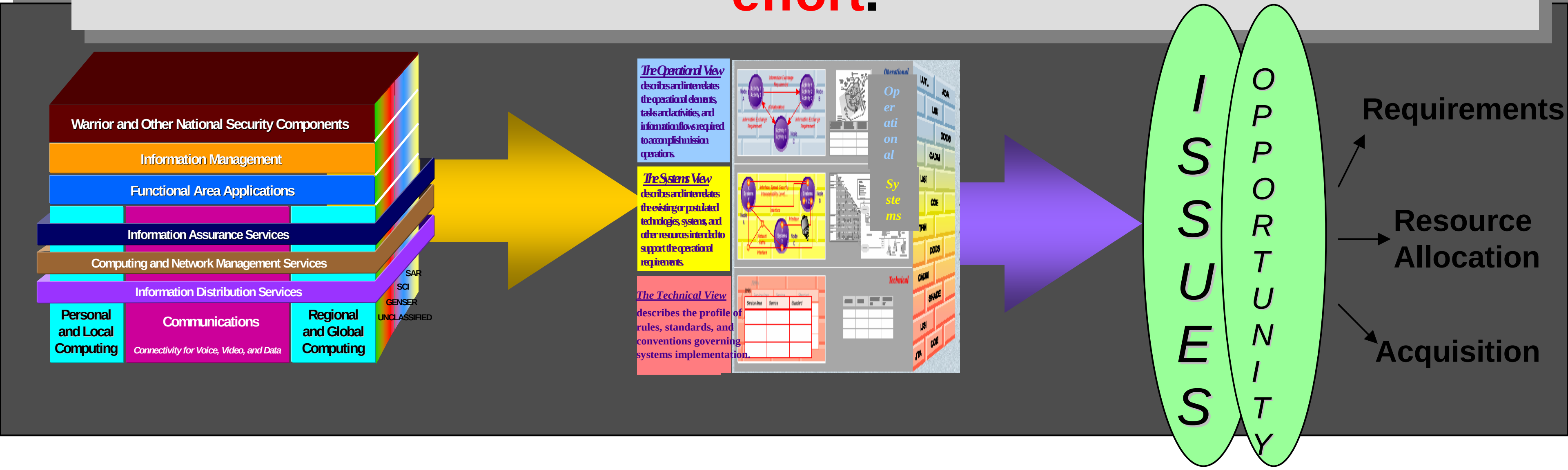
Agenda

back

more

GAIP Action Item

Develop a decision process to prioritize and decide the issues that surface as a result of the GIG architecture effort.



Warrior and Other National Security Components
Information Management
Functional Area Applications
Information Assurance Services
Computing and Network Management Services
Information Distribution Services
Personal and Local Computing
Communications
Connectivity for Voice, Video, and Data
Regional and Global Computing
SAR
SCI
GENSER
UNCLASSIFIED
The Operational View describes and interrelates the operational elements, tasks and activities, and information flows required to accomplish mission operations.
The Systems View describes and interrelates the existing or postulated technologies, systems, and other resources intended to support the operational requirements.
The Technical View describes the profile of rules, standards, and conventions governing systems implementation.
Operational
Systems
Technical
ISSUES
OPPORTUNITY
Requirements
Resource Allocation
Acquisition

RBA/eBusiness and KM Critical Shortfalls

Agenda
back

	People	Policy / Process	Technology / Material
Revolution in Business Affairs	- Defense-wide Perspective - Awareness & Training - Expect Improvement Ideas from bottom and top - Break “rice bowls”	- Shared Business Framework - Legal Framework - Strategic Investment Plan - Resource Visibility	- Measures of Effectiveness - Business Best Practices - Robust GIG
Process Improvement	- Senior Change Champions - Interdisciplinary Skills - Become Change Agents or be change victims - Foster new ideas	- Rapid Change Management - Reward and Encourage Improvements - Common Architectural Understanding - Implementation Guidance	- Best Practices Sharing - Information Sharing - System Modernization - Standards - Engineered Solutions
Knowledge Management	- Knowledge Sharing - Expanded “Ownership” Understanding of Intellectual Capital - Awareness & Training - Employee Incentives for Collaboration	- Information Sharing - Institutionalization of KM - Resource Visibility - Capture & sharing of Best Practices - Integration of Information Management Practices	- Infrastructure Visualization - Sharing Tools - Advanced Search and Categorization Tools
Business Security	- Security Appreciation - Confidence in New Processes	- New Paradigms for Trusted Business - Personnel Security - Legal - Auditor - Functional Teaming - Guidance for Enablement	- Smart Card Fielding - Standards & Tools - Public Key Enablement - Security Common Criteria vis-a-vis FIPS

Interoperability Attributes

Agenda

back more

Interoperability Defined

" The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and use the services to enable them to operate effectively together."

Joint Publication 1-02
(emphasis added)

Challenges Recognized

Network-centric Joint and Coalition operations require unprecedented attention to interoperability

Chronic interoperability shortfalls routinely identified in JTF after action report highlights

Interoperability is now a Key Performance Parameter for new programs - architecture focus was needed

Legacy capabilities present an additional challenge

Large IT services contracts represent a unique opportunity

Incentivizing interoperability is a long standing problem

The DoD CIO is responsible under Title 10 to ensure interoperability across the DoD

"Most of our (coalition) joint operations are an ad hoc group of available and ready land, naval, and air units

What's needed is the ability to assemble the right communications, sensors, databases, command and control and information systems to support each different (C) JTF and to have well established processes and procedures … '

excerpt from Kosovo After Action Report

The legacy process is not meeting the challenges

What Fixes are Required?

•Tie Interoperability requirements to Architecture and associated Information Exchange Requirements (e.g., GIG Architecture, Joint Mission Areas)

•Address interoperability as a “family of systems” issue - not as individual “widgets”

•Recognize the need to achieve balance among legacy, new systems and new concepts

•Integrate both material and non material aspects in solving interoperability problems

•Increase realism and fidelity in tests, exercises and after action reports

•Synchronize and focus DoD decision processes & resources on timely fixes

•Provide limited resources for JROC prioritized, out of cycle fixes

•Improve CINC influence on fix and deploy decision making

Reengineering of the legacy process is needed
to meet requirements of the Clinger-Cohen Act and Title 10

Guiding Steps for Interoperability

Agenda

back

Joint Interoperability

- Manage mission capabilities, not individual systems
- Protect interoperability in every phase of the capability development process
- Clearly define interoperability requirements starting with a CRD for each JMA
- Use architecture as integrating tools
- Make effective use of standards w/o stifling innovation
- Revise the PPBS and acquisition processes to facilitate interoperability and mission capability management
- Provide for compliance testing based on families of systems
- Assess results using outcome-based metrics
- Control family-of-systems configuration and spiral evolution continuously

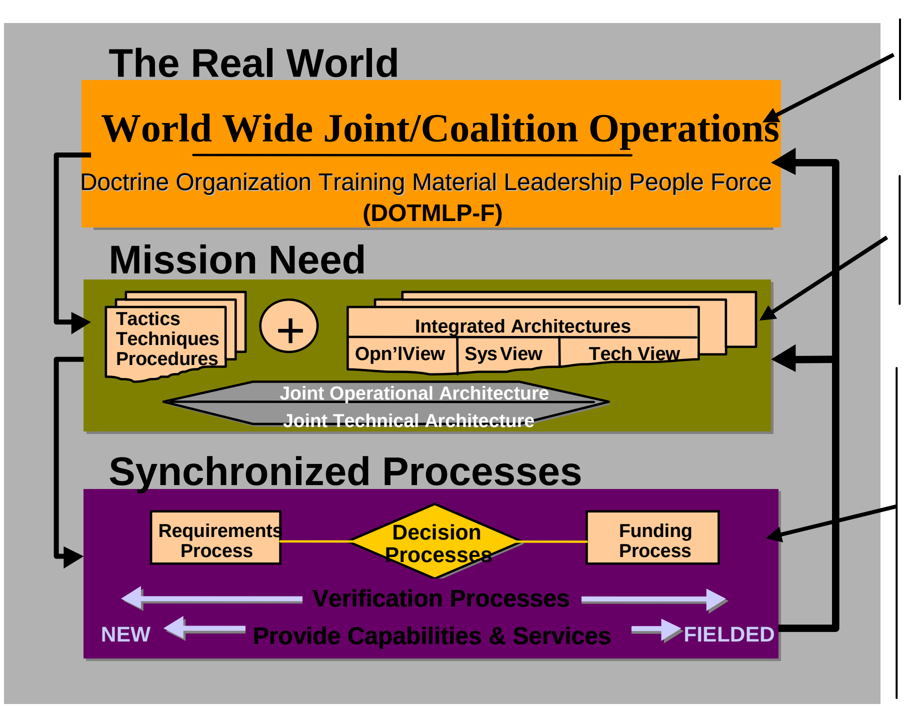
Coalition Interoperability

- Get primary/lead nations to:
  - Agree on core concepts/doctrine
  - Define high level Information Exchange Requirements (IER)
  - Relax information sharing policies reciprocally
- Promulgate the use architectures as integrating tools
- Increase emphasis on non-material aspects of interoperability such as doctrine, training and experimentation
- Exploit commercial technology where appropriate
- Continue to pursue cooperative C4/IM developments where practical
- More effectively coordinate the efforts of the multinational forums addressing multinational interoperability issues

Reengineered Interoperability Process

Agenda
back
more

Key Process Elements & Organizations



The Real World

World Wide Joint/Coalition Operations

Doctrine Organization Training Material Leadership People Force (DOTMLP-F)

Mission Need

Tactics Techniques Procedures

+

Integrated Architectures

Opn'lView | Sys View | Tech View

Joint Operational Architecture

Joint Technical Architecture

Synchronized Processes

Requirements Process

Decision Processes

Funding Process

Verification Processes

NEW

Provide Capabilities & Services

FIELDED

Joint Staff approved Joint Mission Areas

Global Information Grid

Integrated Architectures with IERs

Joint Operational Architecture & JTA

Interoperability as a KPP for new systems

Joint Interoperability Test Bed and Exercises

Joint Integration & Interoperability Organization established at Joint Forces Command

Integrated Material & non Material Decisions

JROC Prioritization w/CIO input

Interoperability Stabilization Fund

Integrated CIO, AT&L and Joint Staff decision making

Initial Resources provided by DepSecDef decision - Sept 1, 2000

Impediments to Interoperability

•Lack of breadth and depth in the family of systems management process - spanning CIO, DAE and CJCS equities

•Potential loss of Joint Staff/J3 sponsorship of the process within the Joint community

•Overlap of responsibilities with the DCI on NFIP capabilities

•Acceptability of architectures by individual program managers

•Complexity of synchronizing decision making on fixes to legacy and new systems

What is Knowledge Management (KM)?

Agenda
back
more

- An integrated & collaborative approach for handling huge volumes of unstructured information flowing within organizations and across the internet:
  - Information and applications
  - Real-time knowledge transfer that provides simultaneous access, analysis, & retrieval
- A course of action to achieve JV2010/JV2020 Information Superiority objectives
- Wide range of new and diverse KM practices and supporting technologies

What have we done to advance KM?

- Organized a DoD-wide KM Community of Interest
- Built KM roadmap, primer, self-assessment guide, core competencies, lessons learned, and a repository of best practices
- Integrated KM & EB programs
- Established the KM support program office (Oct 98) and built reusable Intranet templates
- Created a Data Interoperability Campaign Plan to revamp the DoD Data Administration Program
- Participated in the Federal CIO Council and stay engaged in the KM Special Interest Group

Key KM Initiatives

Agenda
back
more

- US Joint Forces Command “Knowledge Today” enables the 1500 personnel to share knowledge
- USS Stennis Battle Group’s Project provides real-time knowledge transfer, repository of updates and trends, simultaneous BG access, and information analysis, archival, and retrieval
- Army Knowledge On-Line (AKO) and the Land Information Warfare Activity (LIWA) programs provides global portals to share knowledge
- C3I collaborating w/ Acquisition, Military Operations Research, Comptroller, and other communities to aggressively apply KM practices
- CIO Information & Knowledge Exchange (IKE) Portal in beta testing
- Intranet KM templates built by C3I being reused by USJFC, Army, Navy, Marines, Air Force, and several Federal agencies

What must be done to institutionalize KM?

Agenda

back

- Revamp policies and education programs to incorporate KM practices and to deal with privacy and intellectual property rights
- Increase cross-functional and cross-component sharing and cooperation
- Partner with Federal and Industry share lessons learned
- Encourage DoD leaders to:
  - Personally “champion” KM initiatives.
  - Create a vision for KM as it supports your organization’s overall strategy
  - Articulate “guiding principles” for KM to the organization’s knowledge workers
  - Encourage and support creation of communities of interest
- Develop measures of merit for KM to resonate with leaders, managers, and knowledge workers

Cost Base Accounting

Agenda

back more

- What is it?
  - An accounting information system that assigns costs to products based on the resources consumed. It enables managers to identify all the costs of producing particular products and services, providing an accurate, aggregate cost of doing business.
- What are we trying to achieve?
  - An efficient method by which we convert resources into value by determining a competitive price for a product, developing budgets, future cost estimating and measuring performance.

Agenda
back
more

Cost Base Accounting

- What have we achieved?
  - Cost Base Accounting management concept has been around for some years, but recent advances in information Technology provided the capability to better use this approach to identify the real cost of our business practices and use that information to manage more effectively.
  - Pockets of the department are making inroads with this tool, by making effective cost decisions during development and production phases of a program which allows managers to provide quality supplies and services to their customers.
  - A rigorous training effort is underway through the BPR.

Cost Base Accounting

- What are the impediments to progress?
  - – Lack of strong top leadership
  - – Resistance to change
  - – Disconnect between managers and employees in the perception of how the new information is used to resolve problems.
  - – Poor financial management systems
  - – Lack of a department-wide training program.

CIO Authorities

Agenda
back

Sources:

- •Clinger-Cohen Act of 1996
- •Chapter 131 of Title 10, Section 2223, “Additional Information Technology Responsibilities of Chief Information Officers”
- •Paperwork Reduction Act
- •Executive Order 13011, “Federal Information Technology,” dated July 16, 1996
- •SecDef Memo, “Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106), dated June 2, 1997

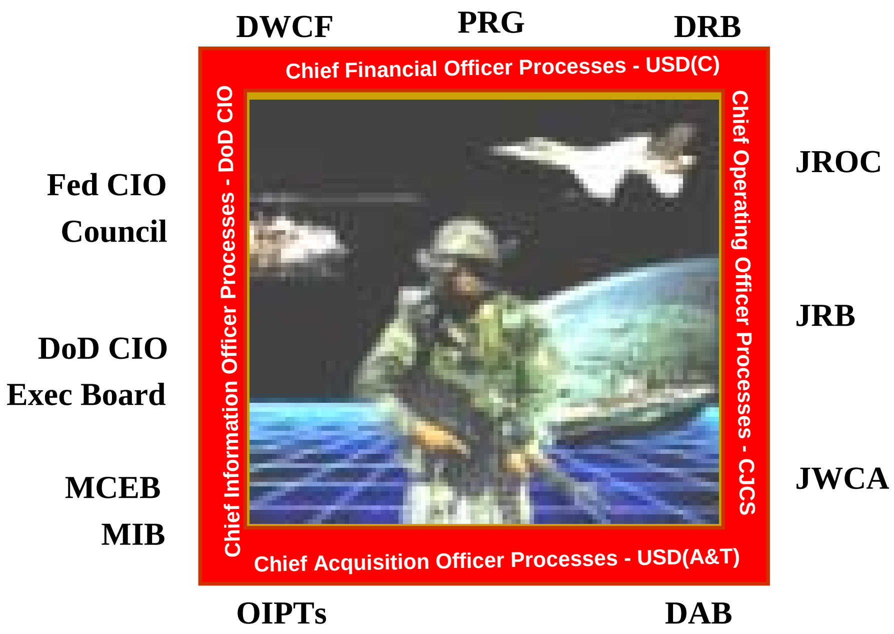
Fundamental Responsibilities:

- •Coordination of information resource management activities
- •Policy development for DoD IM/IT
- •Strategic planning for DoD IM/IT
- •Resource management for IT and NSS (National Security Systems) investments
- •Oversight of all DoD IT programs

Infostructure Visibility

Agenda

back


DWCF
PRG
DRB
Chief Financial Officer Processes - USD(C)
Fed CIO Council
DoD CIO Exec Board
MCEB
MIB
Chief Information Officer Processes - DoD CIO
Chief Operating Officer Processes - CJCS
JROC
JRB
JWCA
Chief Acquisition Officer Processes - USD(A&T)
OIPTs
DAB

•<u>Governance</u>

- •DoD IM Strategic plan
- •GIG Architecture
- •GIG Policy Documents

•<u>Boards and Panels</u>

- •DoD CIO Executive Board
- •Architecture Coordination Council
- •GIG Architecture Integration Panel
- •Pentagon Area IT Oversight Executive Board
- •GIG/Network Waiver Board

System of System Integration

Agenda

back

- Issue:
  - The Department continues to develop and buy weapons and C4ISR systems with limited consideration for integration, interoperability and supportability

- Way Forward:
  - Expand Family of Systems oversight to a Department strategy
  - Review and reconcile Title 10 for inconsistencies re: interoperability
  - Continue the Joint C2 Integration and Interoperability Group examination of legacy systems

Leveraging Commercial Technology

Agenda

back

Issues:

1 - *"Marketing the Marketers" a*nnouncing to a growing commercial Information Technology Sector the needs, plans, challenges, and problems of DoD

2 - Identifying commercial sector technology leaders

3 - DoD Acquisition Practice and IT Management - How to quickly acquire and implement IT technology for the warfighter levels (JTF and below)

5 - Need a core DoD IT professionals to capitalize on commercial technology for DoD needs

Way Forward:

1 - Dissemination of an Interactive *OASD Advanced Technology Roadmap* on the NIPRNET as a tool to "*Market the Marketers*" serve as an initial portal in the creation of the IT Forum

2 - Development of a formalized integrated IT Forum - Service Labs, Joint Battle Center, DARPA, and Service/Joint/DOD Chief Information Officers - Establishing common standards and commercial business service

3- Utilize Commercial Business Practice and Services (Using Vendors) for IT Implementation, Technical Support, and System Upgrades.

Agenda
back
more

C2 Research

- Achieving Information Superiority requires a better understanding of how to
  - extract knowledge from information
  - visualize uncertainty and risk
  - create awareness
  - share awareness
  - collaborate
  - facilitate distributed teams
- Leveraging Information Superiority requires new Command concepts and a better understanding of
  - expressing intent
  - self-synchronization
  - coalition command and control
- We also need a better understanding of how to
  - protect our information and information processes
  - integrate a system of systems

Our current R&D focus is on technology not on its utilization and the coevolution of mission capability packages (DOTMLPF)

C2 Analysis and Modeling

Agenda
back
more

- Analyses and Models support a wide variety of activities that are critical to the success of DoD Transformation efforts (e.g.)

  - Concept Development
  - Investment Decisions
  - Experiments
  - Training and Rehearsal

- Their utility depends upon their ability to represent "reality" and to discriminate among "options"

21st Century Realities include:

- Operation Other than War
- Coalition Operations
- Asymmetrical Warfare

21st Century Options include:

- Information Warfare
- New C2 Approaches
- New Ops Concepts
- Dynamic ROE

- The current generation of models is extremely limited in their ability to represent "reality" and to discriminate among "options"
- The next generation of models does not adequately address these shortfalls

IS Technology Base

Agenda

back

- Issue: Sustaining Information Superiority requires the continual development of information technologies and their rapid insertion of technology

- Way Forward: Development of an advanced IS technology plan
  - information assurance
  - global information grid
  - end to end C3ISR and Space integration
  - knowledge management
  - security
  - information operations
  - intelligence
  - electronic business

Experimentation

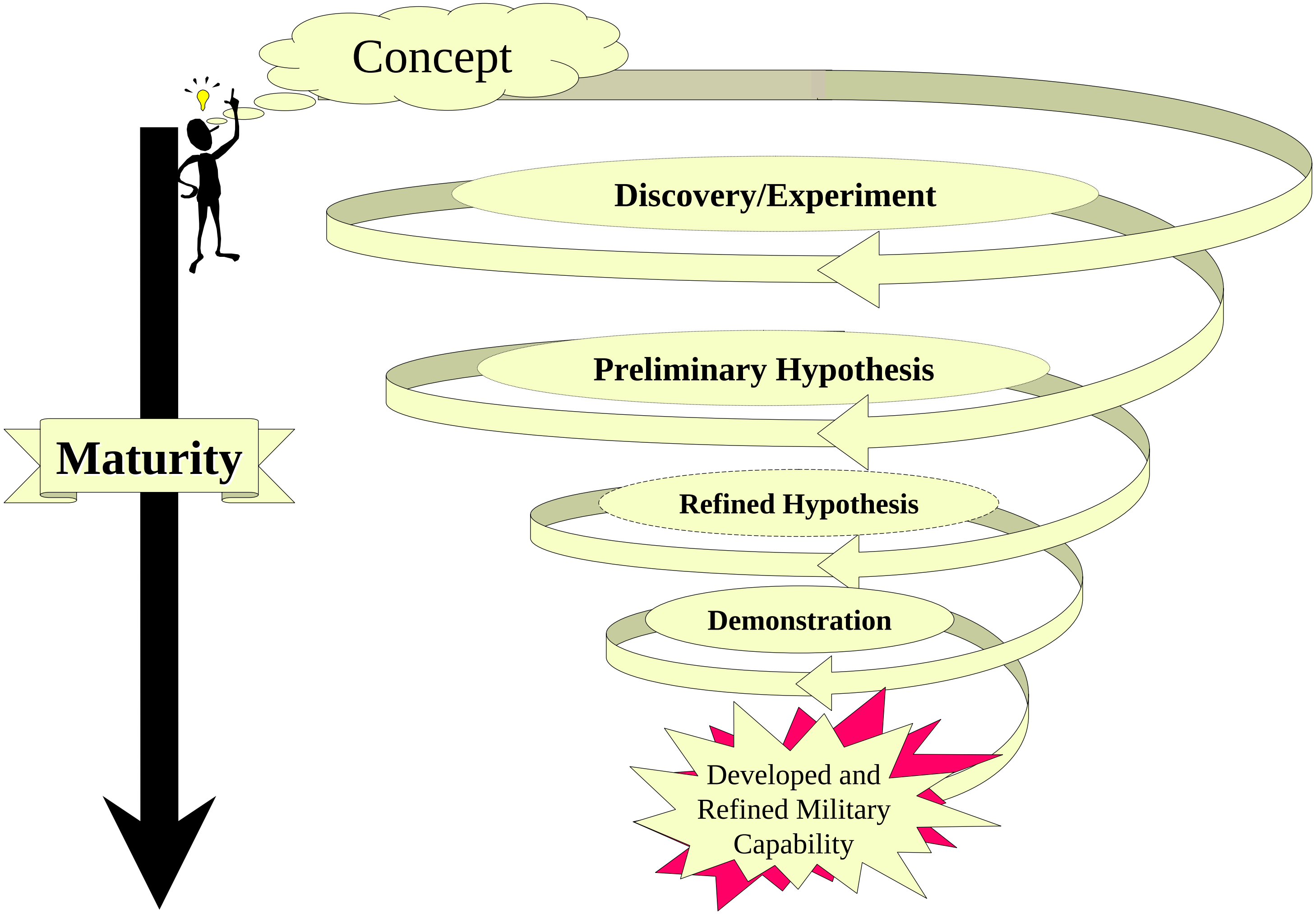
- Experiments are on the Critical Path from Concepts to a Real Operational Capability

- Information Superiority and Network Centric Concepts provide an Organizing Principle for Experimentation that will develop experimental synergies and support transformation

- Lessons from “Experiments” are being Recorded not Learned

- Convergence on a set of metrics is necessary for progress

From Concept to Capability



Agenda

back

more

Organizing Logic for Experimentation

- IS and NCW Concepts Provide an Organizing Logic for Concept-Based Experimentation Based upon
  - Elements of Information Superiority
  - Attributes of a Network-Centric Force
- This Organizing Logic Gives Rise to an Integrated and Coherent Set of
  - Hypotheses
  - Metrics (dependent variables)
  - Key Independent Variables (“treatments” and “conditions”)

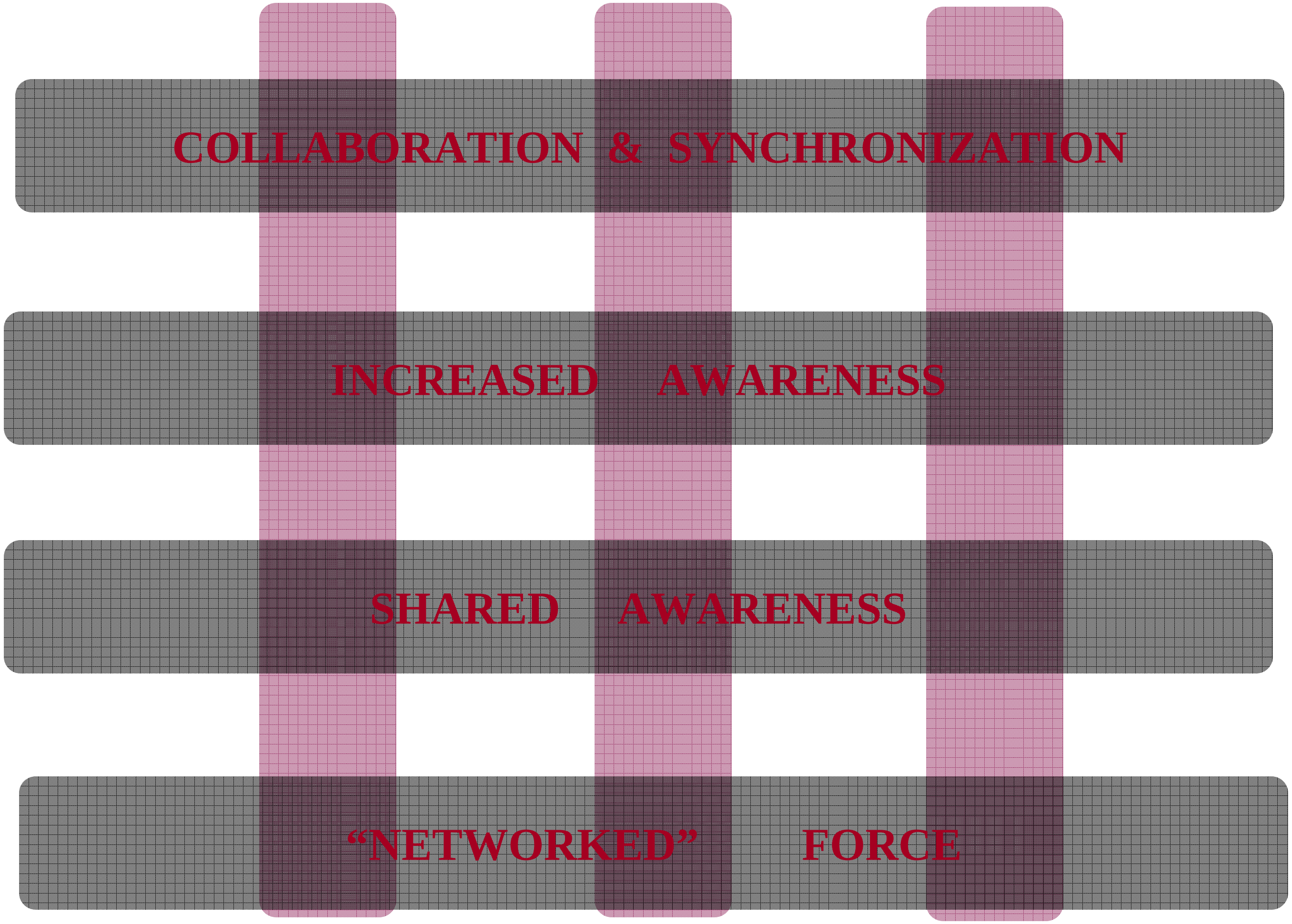
Experimental Space

Agenda

back

more

Mission Capability Packages



COLLABORATION & SYNCHRONIZATION

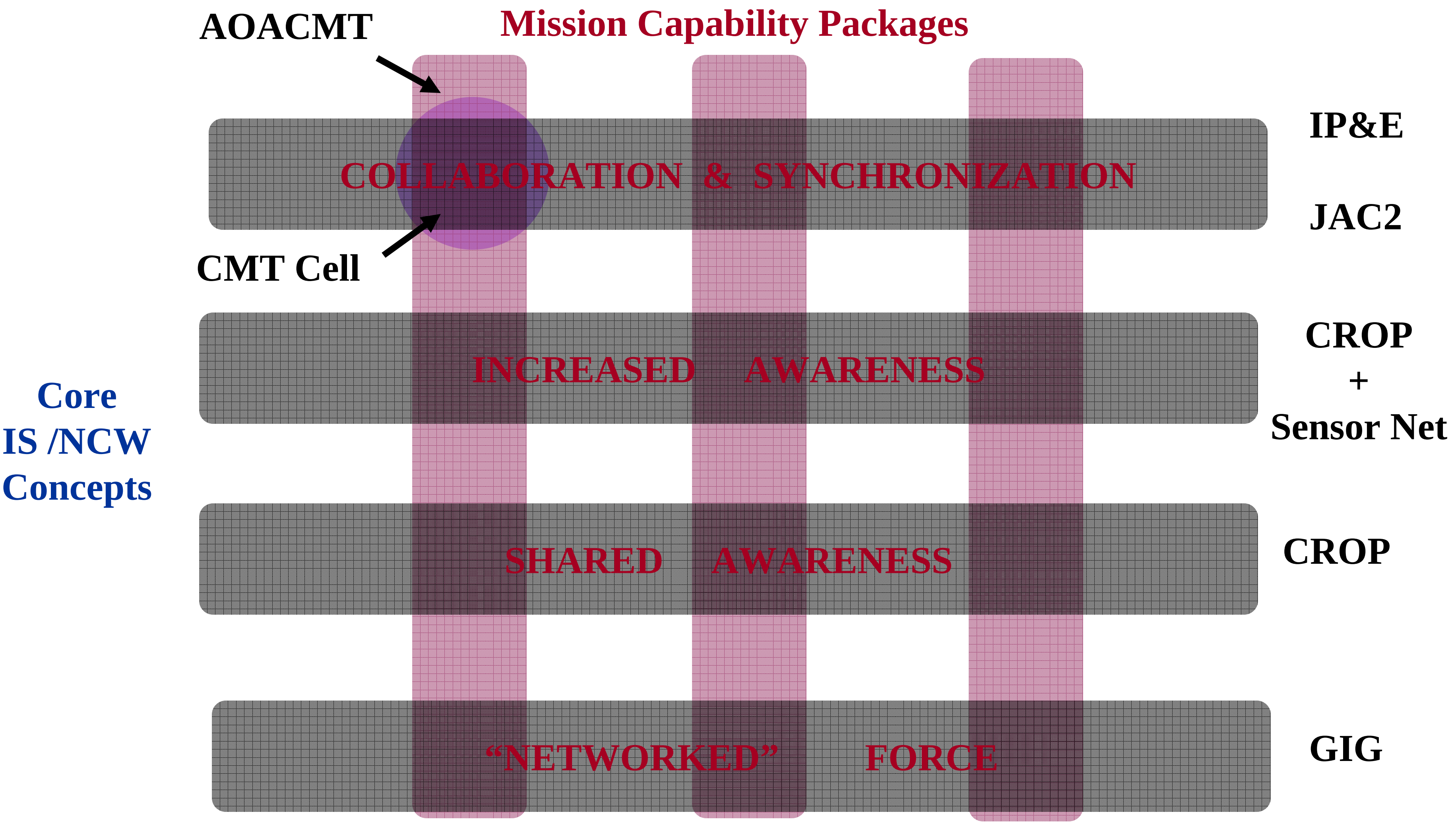
INCREASED AWARENESS

SHARED AWARENESS

“NETWORKED” FORCE

Core
IS / NCW
Concepts

Experimental Space



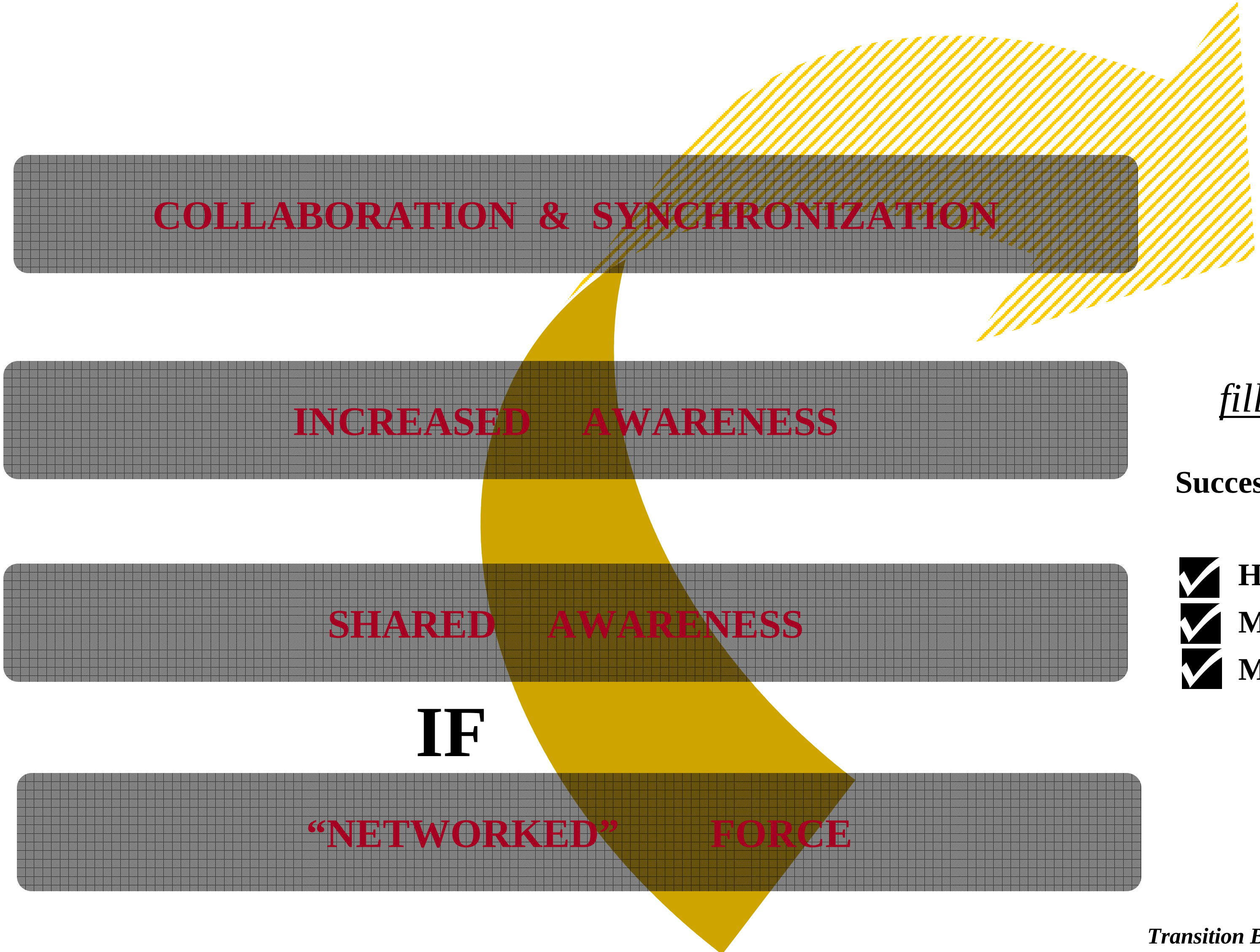
Power of IS / NCW Core Concepts

as Organizing Principle for Experimentation

- They Get at the Fundamentals
- Facilitate Sharing of Experimental Results Across Missions and Contexts
- Enable Creation of a Useful Body of Knowledge
- Bottom Line: More Bang for the Experimental Buck

Agenda
back
more

Hypothesis Template



THEN

COLLABORATION & SYNCHRONIZATION

INCREASED AWARENESS

SHARED AWARENESS

IF

“NETWORKED” FORCE

fill in the mission

Success with

- ☑ **Higher Probability**
- ☑ **More Quickly**
- ☑ **More Efficiently**

The Grand Hypothesis

Goals

-Shape security environment
- Deter aggression or abort conflict
- Deny occupation and defend friendly assets
- Neutralize or degrade an adversary's capabilities
- Across the spectrum of conflict

Enabling

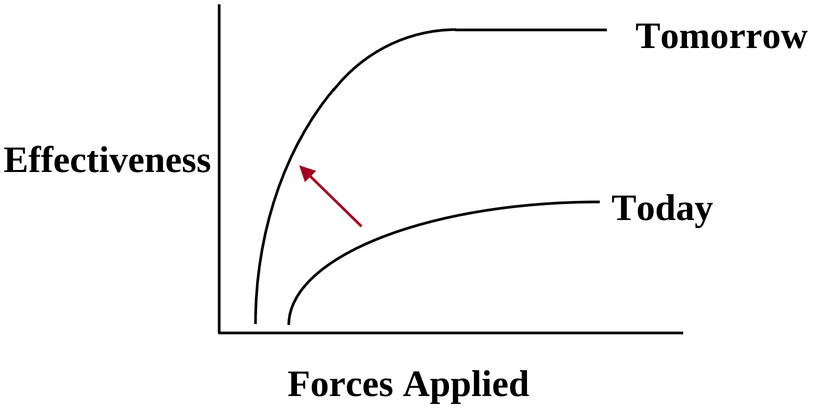
- Preemptively foreclose adversary COA
- Shock and Awe (Paralyze, Shatter, Disintegrate)
- Increased Speed and Lethality
- Reduced Risk and Increased Survivability

NCW Characteristics and Capabilities

-Increased Battlespace Awareness and Knowledge
- Adaptive C2 Approaches and Organizational Structures
- Self-synchronizing Forces

There is a growing body of evidence that

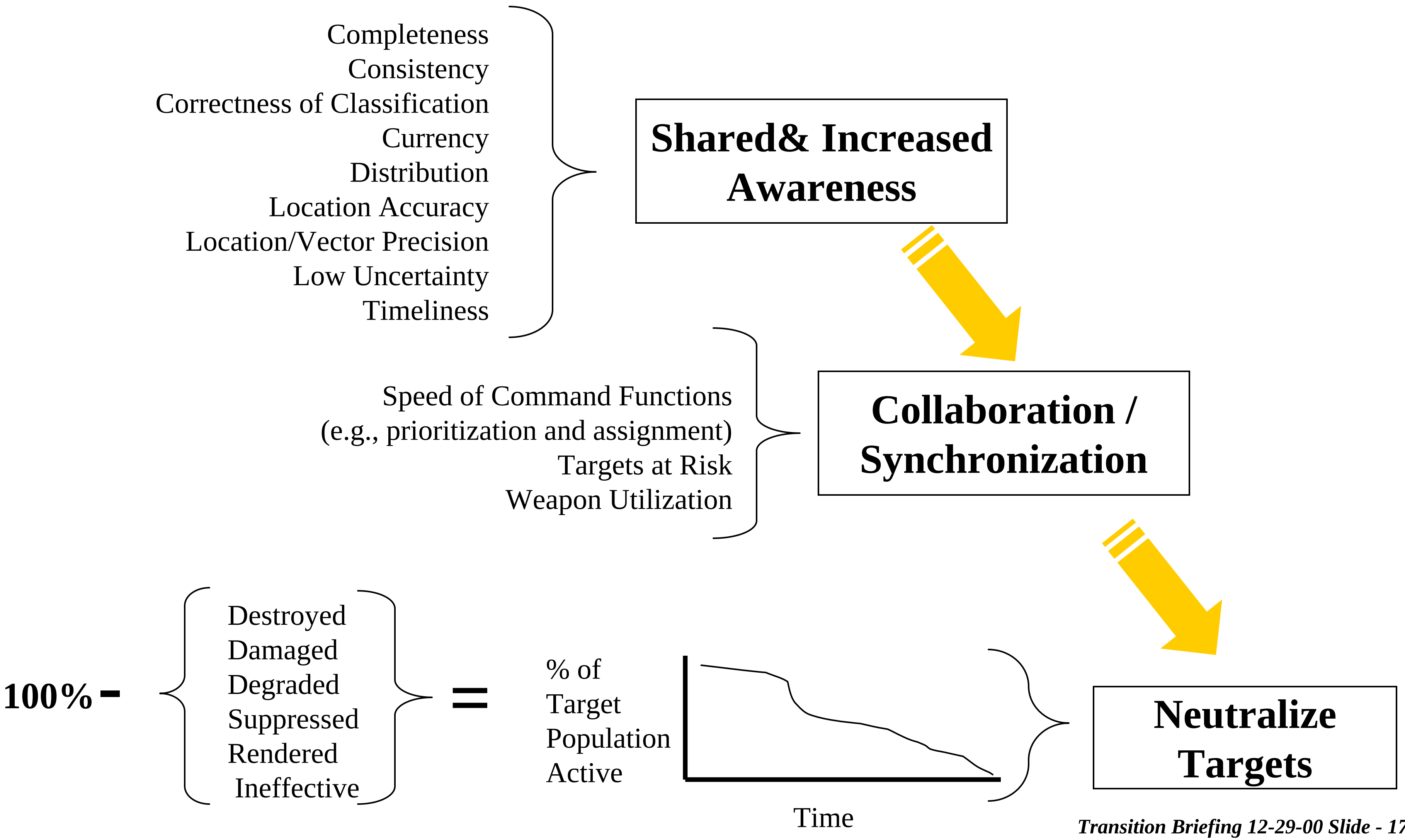
NCW Enables an Isoquantal Shift



Adapted from: "An Evolutionary Cornerstone for JV2010" 3/9/99
prepared for the J6 by Roy Evans

Agenda
back
more

Illustrative Metrics



Completeness
Consistency
Correctness of Classification
Currency
Distribution
Location Accuracy
Location/Vector Precision
Low Uncertainty
Timeliness

Shared& Increased Awareness

Speed of Command Functions
(e.g., prioritization and assignment)
Targets at Risk
Weapon Utilization

Collaboration / Synchronization

100% - Destroyed
Damaged
Degraded
Suppressed
Rendered
Ineffective **=**

Neutralize Targets

Experimentation Lessons “Recorded”

- There is a Learning Curve
  - What Future Technology Can Do
  - How to Co-Evolve MCPs
- The Value of the “Pre” and the “Post”
  - Importance of Focus
  - Value of Analysis
- Projecting Future Technology is Necessary to Stay Ahead of the Power Curve
  - - Information Superiority Advanced Technology Plan

IS-Related Experimentation

Agenda
back

Experimental Issues:

- Appropriate attention to IS-related hypotheses and effects
- Determining the worth of investment in IS for the Warfighter
- Coordinating experimentation efforts, technology, metrics, and sharing of effects within the IS Community
- Integration of Conventional Operations and Information Operations
- Limited nature of planned Allied & Coalition IS Experimentation
- Integration of on-going R&D (DARPA) into experimentation efforts

Way Forward:

- Development of IS metrics for all experimentation environments
- Conduct of IS-LOEs with rigorous experimental design and analyses
- Continued Asymmetrical Warfare Experimentation
- Increased Participation by the Federated Battle Lab for the Coordinating Experimentation Efforts
- Active integration of DARPA efforts into experimentation community

Strategic Planning

- Strategic IS planning is complicated by the way that DoD has traditionally built its budgets and manages its programs
  - Service and program centric
  - Lack of “Cost Accounting”

- To be effective a strategic plan for creating Information Superiority and the conditions necessary for the emergence of network-centric operations needs to address at a minimum
  - end to end connectivity
  - enterprise interoperability
  - integrated protection

Impediments to Progress

Agenda

back

- Progress on Infostructure is Being Constrained by
  - Lack of InfostructureVisibility
  - Inadequate Rqmts Definition
  - Program-Centric Planning
  - Insufficient Integration
  - Delays in Deploying Technology
  - Lack of Joint Systems Commands and Labs
- Progress on Design of Information-Enabled MCPs is Being Constrained by
  - Lack of Understanding of Future Capabilities
  - Lack of Information-Enabled Experimental Venues
  - Lack of Harvesting of “Small” Experiments
- Progress on the Balanced Development of MCPs is Being Constrained by
  - Continued Emphasis on Platform Centric Investments and Concepts
  - Separate and Unequal Treatment of MCP Elements
  - Lack of MCP Visibility and Analysis
  - Failure to Work the Nexus Between Organizations, Doctrine, and Information Technology

Challenges

Agenda

back

Issues / Recommendations

Agenda
back
more

- The current tendency to judge the importance of an issue based upon how much money is involved results in ignoring significant even critical issues

- Focusing on the allocation of marginal dollars can only result in marginal improvements

- The major Information Superiority-related issues are systemic ones that go to the heart of how we determine requirements, set priorities, manage risks, make investment decisions, and manage programs

- These issues are, by and large, strategy independent.

- Priorities for C4ISR investments are, however, affected by strategy but the potential effectiveness of these investments is highly dependent on the way we deal with our systemic issues

Strategy Independent Issues

- DoD commitment to a robust, secure, reliable, interoperable infostructure
- Removal of the Impediments to Progress by
  - Consolidation of requirements, investments, planning, and management of the infostructure to provide visability, direction, and accountability
  - Focus on the co-evolution of network-centric mission capability packages (DOTMLP-F) from concept exploration to development to deployment
  - Expansion of Information Age educational programs, experimental venues, and research initiatives
  - Investment in a new generation of analysis methods and tools that are designed to incorporate and reflect network-centric operations and Information Superiority concepts and metrics.

Strategy Dependent Recommendations

Agenda

back

- Shape, Prepare, and Respond (Status Quo)
  - keep the priorities the same
- Modernization
  - interoperable tactical C2, unmanned ISR, bandwidth, net ops, FIA/TPED
- Engage Today
  - airborne ISR, buy commercial, interoperability fixes
- Transformation
  - process change, confederated intel, spaced-based ISR (MTI)

Drill Down
to be provided